IBM Client Security Solutions

Client Security Version 5.1 mit Tivoli Access Manager verwenden

IBM Client Security Solutions

Client Security Version 5.1 mit Tivoli Access Manager verwenden

Hinweis:
Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten Sie die Informationen in Anhang C, „Bemerkungen und Marken", auf Seite 41, lesen.

- Die IBM Homepage finden Sie im Internet unter: **ibm.com**
- IBM und das IBM Logo sind eingetragene Marken der International Business Machines Corporation.
- Das e-business-Symbol ist eine Marke der International Business Machines Corporation.
- Infoprint ist eine eingetragene Marke der IBM.
- ActionMedia, LANDesk, MMX, Pentium und ProShare sind Marken der Intel Corporation in den USA und/oder anderen Ländern.
- C-bus ist eine Marke der Corollary, Inc. in den USA und/oder anderen Ländern.
- Java und alle auf Java basierenden Marken und Logos sind Marken der Sun Microsystems, Inc. in den USA und/oder anderen Ländern.
- Microsoft Windows, Windows NT und das Windows-Logo sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.
- PC Direct ist eine Marke der Ziff Communications Company in den USA und/oder anderen Ländern.
- SET und das SET-Logo sind Marken der SET Secure Electronic Transaction LLC.
- UNIX ist eine eingetragene Marke der Open Group in den USA und/oder anderen Ländern.
- Marken anderer Unternehmen/Hersteller werden anerkannt.

Erste Ausgabe (April 2003)

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
IBM Client Security Solutions, Using Client Security Software Version 5.1 with Tivoli Access Manager,
herausgegeben von International Business Machines Corporation, USA

© Copyright International Business Machines Corporation 2002
© Copyright IBM Deutschland Informationssysteme GmbH 2003

Informationen, die nur für bestimmte Länder Gültigkeit haben und für Deutschland, Österreich und die Schweiz nicht zutreffen, wurden in dieser Veröffentlichung im Originaltext übernommen.

Möglicherweise sind nicht alle in dieser Übersetzung aufgeführten Produkte in Deutschland angekündigt und verfügbar; vor Entscheidungen empfiehlt sich der Kontakt mit der zuständigen IBM Geschäftsstelle.

Änderung des Textes bleibt vorbehalten.

Herausgegeben von:
SW TSC Germany
Kst. 2877
April 2003

Inhaltsverzeichnis

Vorwort

Das vorliegende Handbuch enthält nützliche Informationen für die Konfiguration von Client Security für die Verwendung mit IBM Tivoli Access Manager.

Das Handbuch ist wie folgt aufgebaut:

Kapitel 1, „**Einführung in IBM Client Security**", enthält eine Übersicht über die in der Software enthaltenen Anwendungen und Komponenten sowie eine Beschreibung der PKI-Funkionen (Public Key Infrastructure).

Kapitel 2, „Client Security-Komponente auf einem Tivoli Access Manager-Server installieren", enthält die Voraussetzungen und Anweisungen für die Installation von Client Security auf dem Tivoli Access Manager-Server.

Kapitel 3, „IBM Clients konfigurieren", enthält die notwendigen Informationen und Anweisungen für die Konfiguration von IBM Clients für die Verwendung der Authentifizierungsservices von Tivoli Access Manager.

Kapitel 4, „Fehlerbehebung", enthält nützliche Informationen zur Fehlerbehebung, die beim Befolgen der in diesem Handbuch enthaltenen Anweisungen auftreten können.

Anhang A, „Regeln für Kennwörter und Verschlüsselungstexte", enthält Kriterien für Kennwörter, die auf einen UVM-Verschlüsselungstext angewendet werden können, und Regeln für Kennwörter für den IBM Security Chip.

Anhang B, „Regeln für den UVM-Schutz für die Anmeldung am System", enthält Informationen zur Verwendung des UVM-Schutzes für die Anmeldung am Betriebssystem.

Anhang C, „Bemerkungen und Marken", enthält Informationen zu rechtlichen Hinweisen und Marken.

Zielgruppe

Das vorliegende Handbuch wendet sich an Administratoren des Unternehmens, die mit Tivoli Access Manager Version 3.8 und Version 3.9 auf einem IBM Client Authentifizierungsobjekte verwalten, die mit der UVM-Sicherheits-Policy (User Verification Manager) konfiguriert sind.

Die Administratoren müssen mit den folgenden Begriffen und Verfahren vertraut sein:

- Installation und Verwaltung des SecureWay Directory-LPAP-Protokolls (Lightweight Directory Access Protocol)
- Installations- und Konfigurationsverfahren für Tivoli Access Manager Runtime Environment
- Verwaltung des Tivoli Access Manager-Objektbereichs

Benutzung des Handbuchs

Mit dem vorliegenden Handbuch können Sie die Client Security-Unterstützung für Tivoli Access Manager konfigurieren. Das Handbuch ist eine Ergänzung zu den Veröffentlichungen *Client Security Installationshandbuch*, *Client Security Administratorhandbuch* und *Client Security Benutzerhandbuch*.

Das Handbuch und die gesamte Dokumentation zu Client Security kann von der IBM Website unter http://www.pc.ibm.com/ww/security/secdownload.html heruntergeladen werden.

Verweise auf das *Client Security Installationshandbuch*

Das vorliegende Handbuch enthält Verweise auf das *Client Security Installationshandbuch*. Nachdem auf dem Client der Tivoli Access Manager-Server installiert und konfiguriert wurde und die Runtime Environment installiert wurde, können Sie mit Hilfe der Anweisungen im *Client Security Installationshandbuch* Client Security auf IBM Clients installieren. Weitere Informationen können Sie Kapitel 3, „IBM Clients konfigurieren”, auf Seite 9, entnehmen.

Verweise auf das *Client Security Administratorhandbuch*

Das vorliegende Handbuch enthält Verweise auf das *Client Security Administratorhandbuch*. Das *Client Security Administratorhandbuch* enthält Informationen dazu, wie für den IBM Client Benutzerauthentifizierung und UVM-Policy eingerichtet werden. Nach der Installation von Client Security können Sie mit Hilfe der Anweisungen im *Client Security Administratorhandbuch* die Benutzerauthentifizierung und Sicherheits-Policy einrichten. Weitere Informationen können Sie Kapitel 3, „IBM Clients konfigurieren”, auf Seite 9, entnehmen.

Zusätzliche Informationen

Zusätzliche Informationen sowie Aktualisierungen für Sicherheitsprodukte können, wenn erhältlich, von der IBM Website unter http://www.pc.ibm.com/ww/security/securitychip.html heruntergeladen werden.

Kapitel 1. Einführung in IBM Client Security

Die Software ″IBM Client Security″ ist für IBM Computer konzipiert, die den integrierten IBM Security Chip zum Verschlüsseln von Dateien und Speichern von Chiffrierschlüsseln verwenden. Client Security besteht aus Anwendungen und Komponenten, mit denen IBM Kunden die Sicherheit von Clients im lokalen Netzwerk, im Unternehmen oder im Internet gewährleisten können.

Anwendungen und Komponenten von Client Security

Wenn Sie Client Security installieren, werden die folgenden Softwareanwendungen und -komponenten installiert:

- **Administratordienstprogramm:** Das Administratordienstprogramm ist die Schnittstelle, über die ein Administrator den integrierten IBM Security Chip aktiviert oder inaktiviert sowie Chiffrierschlüssel und Verschlüsselungstexte erstellt, archiviert und erneut generiert. Darüber hinaus kann ein Administrator mit diesem Dienstprogramm der Sicherheits-Policy, die von Client Security bereitgestellt wird, Benutzer hinzufügen.
- **User Verification Manager (UVM):** In Client Security werden mit UVM Verschlüsselungstexte und andere Elemente verwaltet, mit denen Systembenutzer authentifiziert werden. Mit einem Lesegerät für Fingerabdrücke kann UVM z. B. bei der Anmeldung Benutzer authentifizieren. UVM bietet folgende Möglichkeiten:
  - **Schutz durch UVM-Client-Policy:** Mit UVM kann ein Administrator die Sicherheits-Policy für Clients festlegen, die bestimmt, wie auf dem System die Authentifizierung eines Clientbenutzers erfolgt.

    Wenn die Policy festlegt, dass Fingerabdrücke für die Anmeldung erforderlich sind, und der Benutzer keine Fingerabdrücke registriert hat, hat er die Möglichkeit, Fingerabdrücke bei der Anmeldung zu registrieren. Wenn die Überprüfung von Fingerabdrücken erforderlich ist und kein Scanner angeschlossen ist, meldet UVM einen Fehler. Wenn das Windows-Kennwort nicht oder nicht richtig in UVM registriert ist, hat der Benutzer die Möglichkeit, das richtige Windows-Kennwort als Teil der Anmeldung anzugeben.
  - **UVM-Systemanmeldeschutz:** UVM ermöglicht es Administratoren, den Zugriff auf die Computer über eine Anmeldeschnittstelle zu steuern. Der UVM-Schutz stellt sicher, dass nur Benutzer, die von der Sicherheits-Policy erkannt werden, auf das Betriebssystem zugreifen können.
  - **UVM Client Security-Bildschirmschonerschutz:** Bei Einsatz von UVM können Benutzer den Zugriff auf den Computer über eine Schnittstelle für den Client Security-Bildschirmschoner steuern.
- **Administratorkonsole:** Die Administratorkonsole von Client Security ermöglicht es einem Sicherheitsadministrator, administratorspezifische Tasks über Fernzugriff auszuführen.
- **Benutzerkonfigurationsprogramm:** Mit dem Benutzerkonfigurationsprogramm können Clientbenutzer den UVM-Verschlüsselungstext ändern. Unter Windows 2000 und Windows XP können Benutzer mit dem Clientdienstprogramm Schlüsselarchive aktualisieren und Windows-Anmeldekennwörter ändern, so dass diese von UVM erkannt werden. Außerdem kann ein Benutzer Sicherungskopien der digitalen Zertifikate erstellen, die vom integrierten IBM Security Chip erzeugt wurden.

PKI-Funktionen

Client Security bietet alle erforderlichen Komponenten, um in Ihrem Unternehmen eine PKI (Public Key Infrastructure) aufzubauen, z. B.:

- **Steuerung der Client-Sicherheits-Policy durch Administratoren:** Die Authentifizierung von Endbenutzern auf Clientebene ist ein wichtiger Aspekt für Sicherheits-Policies. Client Security bietet die erforderliche Schnittstelle zur Verwaltung der Sicherheits-Policy eines IBM Clients. Diese Schnittstelle ist Teil der Authentifizierungssoftware UVM (User Verification Manager), der Hauptkomponente von Client Security.
- **Chiffrierschlüsselverwaltung für öffentliche Schlüssel:** Administratoren können mit Client Security Chiffrierschlüssel für die Computerhardware und für die Clientbenutzer erstellen. Bei der Erstellung von Chiffrierschlüsseln sind diese über eine Schlüsselhierarchie an den integrierten IBM Security Chip gebunden. In der Hierarchie wird ein Hardwareschlüssel der Basisebene verwendet, um die übergeordneten Schlüssel sowie die den einzelnen Clientbenutzern zugeordneten Benutzerschlüssel zu verschlüsseln. Die Verschlüsselung und Speicherung von Schlüsseln auf dem integrierten IBM Security Chip erweitert die Clientsicherheit um eine wesentliche zusätzliche Ebene, da die Schlüssel sicher an die Computerhardware gebunden sind.
- **Erstellung und Speicherung digitaler Signaturen, die durch den integrierten IBM Security Chip geschützt sind:** Wenn Sie ein digitales Zertifikat anfordern, das für die digitale Signatur und für die Verschlüsselung einer E-Mail verwendbar ist, können Sie mit Client Security den integrierten IBM Security Chip zur Bereitstellung der Verschlüsselung für Anwendungen einsetzen, die mit der Microsoft CryptoAPI funktionieren. Zu diesen Anwendungen gehören Internet Explorer und Microsoft Outlook Express. Dadurch ist sichergestellt, dass der private Schlüssel des digitalen Zertifikats auf dem integrierten IBM Security Chip gespeichert wird. Darüber hinaus können Netscape-Benutzer integrierte IBM Security Chips zum Generieren von privaten Schlüsseln für die zum Erhöhen der Systemsicherheit verwendeten digitalen Zertifikate auswählen. Anwendungen nach dem Standard PKCS #11 (Public-Key Cryptography Standard Nr. 11), wie z. B. Netscape Messenger, können sich über den integrierten IBM Security Chip schützen.
- **Digitale Zertifikate auf den integrierten IBM Security Chip übertragen:** Mit dem Tool zur Übertragung von Zertifikaten von Client Security können Sie Zertifikate, die mit dem Standard-Microsoft-CSP erstellt wurden, an das CSP-Modul des integrierten IBM Sicherheits-Subsystems übertragen. Dadurch wird der notwendige Schutz für private Schlüssel, die zu Zertifikaten gehören, beträchtlich erhöht, da die Schlüssel nun statt in gefährdeter Software im integrierten IBM Security Chip sicher gespeichert sind.
- **Funktion zur Schlüsselarchivierung und -wiederherstellung:** Eine wichtige PKI-Funktion ist das Erstellen eines Schlüsselarchivs, aus dem Schlüssel bei Verlust oder Beschädigung der Originalschlüssel wiederhergestellt werden können. Client Security bietet eine Schnittstelle, mit der Sie mit dem integrierten IBM Security Chip erstellte Archive für Schlüssel und digitale Zertifikate erstellen und diese Schlüssel und Zertifikate bei Bedarf wiederherstellen können.
- **Verschlüsselung von Dateien und Ordnern:** Die Verschlüsselung von Dateien und Ordnern ermöglicht dem Benutzer das schnelle und einfache Ver- und Entschlüsseln von Dateien und Ordnern. So wird eine höhere Stufe von Datensicherheit als erste der Sicherheitsmaßnahmen des CSS-Systems gewährleistet.

- **Authentifizierung über Fingerabdrücke:** IBM Client Security unterstützt das Lesegerät für Fingerabdrücke von Targus als PC-Karte oder über USB für die Authentifizierung. Die Client Security-Software muss installiert sein, bevor die Einheitentreiber für das Targus-Lesegerät für Fingerabdrücke installiert werden, damit ein ordnungsgemäßer Betrieb gewährleistet ist.
- **Smartcard-Authentifizierung:** IBM Client Security unterstützt jetzt auch Smartcards als Authentifizierungseinheiten. Client Security ermöglicht die Verwendung von Smartcards zur Authentifizierung als Token, d. h., es kann sich jeweils nur ein Benutzer authentifizieren. Jede Smartcard ist systemgebunden, wenn nicht der standortunabhängige Zugriff (Roaming) mit Berechtigungsnachweis verwendet wird. Wenn eine Smartcard erforderlich ist, sollte die Systemsicherheit erhöht werden, da diese Karte mit einem Kennwort geliefert werden muss, das möglicherweise ausspioniert werden kann.
- **Standortunabhängiger Zugriff mit Berechtigungsnachweis:** Der standortunabhängige Zugriff mit Berechtigungsnachweis ermöglicht es einem von UVM autorisierten Benutzer, jedes System im Netzwerk genau wie die eigene Workstation zu verwenden. Wenn ein Benutzer berechtigt ist, UVM auf irgendeinem bei CSS registrierten Client zu verwenden, kann er seine persönlichen Daten in alle anderen registrierten Clients im Netzwerk importieren. Die persönlichen Daten werden im CSS-Archiv und auf jedem System, in das sie importiert wurden, automatisch aktualisiert und gewartet. Aktualisierungen der persönlichen Daten, wie z. B. neue Zertifikate oder Änderungen am Verschlüsselungstext, sind sofort auf allen Systemen verfügbar.
- **FIPS 140-1-Zertifizierung:** Client Security unterstützt FIPS 140-1-zertifizierte, verschlüsselte Bibliotheken. FIPS-zertifizierte RSA-BSAFE-Bibliotheken werden auf TCPA-Systemen verwendet.
- **Ablauf des Verschlüsselungstexts:** Client Security legt jeweils beim Hinzufügen eines Benutzers einen benutzerspezifischen Verschlüsselungstext und eine Policy für das Ablaufen des Verschlüsselungstexts fest.
- **Automatischer Schutz für ausgewählte Ordner:** Die Funktion zum automatischen Schützen von Ordnern ermöglicht es einem Client-Security-Administrator, festzulegen, dass alle Ordner mit der Bezeichnung "Eigene Dateien" der von UVM autorisierten Benutzer automatisch geschützt werden, ohne dass seitens der Benutzer eine Aktivität ausgeführt werden muss.

Kapitel 2. Client Security-Komponente auf einem Tivoli Access Manager-Server installieren

Die Authentifizierung von Endbenutzern auf der Clientebene ist ein wichtiger Sicherheitsaspekt. Client Security stellt die Schnittstelle zur Verfügung, die zum Verwalten der Sicherheits-Policy auf einem IBM Client erforderlich ist. Diese Schnittstelle ist Teil der Authentifizierungsoftware User Verification Manager (UVM), die die Hauptkomponente von Client Security darstellt.

Für die Verwaltung der UVM-Sicherheits-Policy für einen IBM Client stehen zwei Methoden zur Verfügung:

- Lokale Verwaltung über den Policy-Editor, der sich auf dem IBM Client befindet
- Unternehmensweite Verwaltung über Tivoli Access Manager

Damit Client Security mit Tivoli Access Manager verwendet werden kann, muss die Client Security-Komponente von Tivoli Access Manager installiert werden. Diese Komponente kann über die IBM Website unter der Adresse http://www.pc.ibm.com/ww/security/secdownload.html heruntergeladen werden.

Voraussetzungen

Damit eine gesicherte Verbindung zwischen dem IBM Client und dem Tivoli Access Manager-Server hergestellt werden kann, müssen die folgenden Komponenten auf dem IBM Client installiert werden:

- IBM Global Security Toolkit
- IBM SecureWay Directory Client
- Tivoli Access Manager Runtime Environment

Weitere Informationen zur Installation und Benutzung von Tivoli Access Manager können Sie der Dokumentation auf der Website unter der Adresse http://www.tivoli.com/products/index/secureway_policy_dir/index.htm entnehmen.

Client Security-Komponente herunterladen und installieren

Die Client Security-Komponente kann gebührenfrei von der IBM Website heruntergeladen werden.

Gehen Sie wie folgt vor, um die Client Security-Komponente herunterzuladen und auf dem Tivoli Access Manager-Server und dem IBM Client zu installieren:

1. Vergewissern Sie sich anhand der Informationen auf der Website, dass Ihr System über den integrierten IBM Security Chip verfügt, indem Sie Ihre Modellnummer mit den Angaben in der Tabelle mit den Systemvoraussetzungen vergleichen. Klicken Sie anschließend auf **Continue**.
2. Wählen Sie den Radioknopf für Ihren Maschinentyp, und klicken Sie auf **Continue**.

3. Erstellen Sie eine Benutzer-ID, füllen Sie das Onlineformular zur Registrierung aus, und lesen Sie die Lizenzvereinbarung. Klicken Sie dann auf **Accept Licence**.

   Sie werden danach automatisch zur Download-Seite für Client Security geführt.
4. Befolgen Sie die angezeigten Anweisungsschritte, um die erforderlichen Einheitentreiber, Readme-Dateien, Software, Referenzdokumente und zusätzliche Dienstprogramme herunterzuladen.
5. Gehen Sie wie folgt vor, um Client Security zu installieren:
   a. Klicken Sie auf dem Windows-Desktop auf **Start > Ausführen**.
   b. Geben Sie in das Feld ″Ausführen″ `d:\verzeichnis\csec50.exe` ein. Hierbei gibt d:\verzeichnis\ den Laufwerkbuchstaben und das Verzeichnis an, in dem die Datei gespeichert ist.
   c. Klicken Sie auf **OK**.

      Das Begrüßungsfenster des InstallShield-Assistenten von IBM Client Security wird angezeigt.
   d. Klicken Sie auf **Weiter**.

      Der Assistent extrahiert die Dateien und installiert die Software. Nach Abschluss der Installation werden Sie gefragt, ob der erforderliche Neustart sofort oder zu einem späteren Zeitpunkt durchgeführt werden soll.
   e. Wählen Sie den entsprechenden Radioknopf aus, und klicken Sie auf **OK**.
6. Klicken Sie nach dem Neustart auf dem Windows-Desktop auf **Start > Ausführen**.
7. Geben Sie in das Feld ″Ausführen″ `d:\verzeichnis\TAMCSS.exe` ein. Hierbei gibt d:\verzeichnis\ den Laufwerkbuchstaben und das Verzeichnis an, in dem die Datei gespeichert ist. Klicken Sie auf **Durchsuchen**, wenn Sie die Datei auswählen möchten.
8. Klicken Sie auf **OK**.
9. Geben Sie einen Zielordner an, und klicken Sie auf **Unzip**.

   Der Assistent extrahiert die Dateien in den angegebenen Ordner. Eine Nachricht teilt mit, dass die Dateien erfolgreich dekomprimiert wurden.
10. Klicken Sie auf **OK**.

Client Security-Komponenten auf dem Tivoli Access Manager-Server hinzufügen

Beim Dienstprogramm ″pdadmin″ handelt es sich um ein Befehlszeilentool, mit dem der Administrator die meisten Tivoli Access Manager-Verwaltungstasks durchführen kann. Die Funktion zur Ausführung mehrerer Befehle ermöglicht es dem Administrator, über eine Datei, die mehrere pdadmin-Befehle enthält, eine vollständige Task oder eine Reihe von Tasks auszuführen. Die Kommunikation zwischen dem Dienstprogramm ″pdadmin″ und dem Verwaltungsserver (pdmgrd) wird über SSL gesichert. Das Dienstprogramm ″pdadmin″ wird als Teil des Runtime Environment-Pakets von Tivoli Access Manager installiert.

Das Dienstprogramm ″pdadmin″ akzeptiert ein Argument für einen Dateinamen, das die Position einer solchen Datei angibt, z. B.:

```
MSDOS>pdadmin [-a <Administrator >][-p <Kennwort >]<Dateiname_mit_Pfad >
```

Der folgende Befehl ist ein Beispiel dafür, wie auf dem Tivoli Access Manager-Server der Objektbereich für IBM Solutions, Client Security Actions und einzelne ACL-Einträge erstellt werden können:

```
MSDOS>pdadmin -a sec_master -p password C:\TAM_Add_ClientSecurity.txt
```

Weitere Informationen zum Dienstprogramm ″pdadmin″ und zu der Befehlssyntax können Sie dem *Tivoli Access Manager Base Administrator Guide* entnehmen.

Gesicherte Verbindung zwischen dem IBM Client und dem Tivoli Access Manager-Server aufbauen

Für den IBM Client muss innerhalb der gesicherten Tivoli Access Manager-Domäne eine eigene authentifizierte Identität aufgebaut werden, um vom Tivoli Access Manager Authorization Service Autorisierungsentscheidungen anfordern zu können.

In der gesicherten Tivoli Access Manager-Domäne muss für die Anwendung eine eindeutige Identität erstellt werden. Damit für die authentifizierte Identität Authentifizierungsüberprüfungen durchgeführt werden können, muss die Anwendung zur Gruppe der fernen ACL-Benutzer gehören. Wenn die Anwendung auf einen der Services der gesicherten Domäne zugreifen möchte, muss sie sich erst an der gesicherten Domäne anmelden.

Das Dienstprogramm ″svrsslcfg″ ermöglicht es IBM Client Security-Anwendungen, mit dem Tivoli Access Manager-Verwaltungsserver und -Autorisierungsserver zu kommunizieren.

Das Dienstprogramm ″svrsslcfg″ ermöglicht es IBM Client Security-Anwendungen, mit dem Tivoli Access Manager-Verwaltungsserver und -Autorisierungsserver zu kommunizieren.

Das Dienstprogramm ″svrsslcfg″ führt die folgenden Tasks aus:

- Erstellt für die Anwendung eine Benutzeridentifikation. Beispiel: DemoUser/HOSTNAME
- Erstellt eine SSL-Schlüsseldatei für diesen Benutzer. Beispiel: DemoUser.kdb und DemoUser.sth
- Fügt den Benutzer der Gruppe der fernen ACL-Benutzer hinzu.

Die folgenden Parameter werden benötigt:

- **-f cfg_file** Name und Pfad der Konfigurationsdatei. Verwenden Sie TAMCSS-.conf
- **-d kdb_dir** Das Verzeichnis, das die Schlüsselringdatenbankdateien für den Server enthalten soll.
- **-n Servername** Der aktuelle Windows-Benutzername/UVM-Benutzername des gewünschten IBM Client-Benutzers.
- **-P admin_pwd** Das Tivoli Access Manager-Administratorkennwort.
- **-s server_type** Es muss ″fern″ angegeben werden.
- **-S server_pwd** Das Kennwort für den neu erstellten Benutzer. Hierbei handelt es sich um einen erforderlichen Parameter.

- **-r port_num** Die empfangsbereite Anschlussnummer für den IBM Client. Dabei handelt es sich um den in der Tivoli Access Manager Runtime-Variablen ″SSL Server Port for PD Management Server″ (SSL Serveranschluss für PD-Verwaltungsserver) angegebenen Parameter.
- **-e pwd_life** Verfallszeit des Kennworts in Anzahl an Tagen.

Gehen Sie wie folgt vor, um eine gesicherte Verbindung zwischen dem IBM Client und dem Tivoli Access Manager-Server aufzubauen:

1. Erstellen Sie ein Verzeichnis, und verschieben Sie die Datei TAMCSS.conf in das neue Verzeichnis.

   Beispiel: `MSDOS> mkdir C:\TAMCSS MSDOS> move C:\TAMCSS.conf C:\TAMCSS\`
2. Führen Sie ″svrsslcfg″ aus, um den Benutzer zu erstellen.

   MSDOS> svrsslcfg -config -f C:\TAMCSS\TAMCSS.conf -d C:\TAMCSS\ -n <server_name> - s remote -S <Serverkennwort> -P <Administratorkennwort> -e 365 -r 199

   Anmerkung: Geben Sie für <Servername> den gewünschten UVM-Benutzernamen und Hostnamen des IBM Clients an. Beispiel: –n DemoUser/MyHostName. Den IBM Client-Hostnamen können Sie herausfinden, indem Sie in die MSDOS-Befehlszeile "hostname" eingeben. Das Dienstprogramm ″svrsslcfg″ erstellt dann auf dem Tivoli Access Manager-Server einen gültigen Eintrag und stellt eine eindeutige SSL-Schlüsseldatei für verschlüsselte Übertragung zur Verfügung.
3. Führen Sie ″svrsslcfg″ aus, um die Position von ivacld der Datei TAMCSS.conf hinzuzufügen.

   Standardmäßig ist beim PD-Autorisierungsserver der Anschluss 7136 empfangsbereit. Sie können das über den Parameter ″tcp_req_port″ in der Zeilengruppe ″ivacld″ der Datei ″ivacld.conf″ auf dem Tivoli Access Manager-Server überprüfen. Es ist wichtig, dass Sie den richtigen ivacld-Hostnamen eingeben. Diese Information können Sie über den Befehl ″pdadmin server list″ anfordern. Die Server wie folgt angeben: <Servername>-<Hostname>. Beispiel für den Befehl ″pdadmin server list″:

```
MSDOS> pdadmin server list ivacld-MyHost.ibm.com
```

Mit dem folgenden Befehl wird anschließend ein Replikatseintrag für den oben angezeigten ivacld-Server hinzugefügt. Es wird davon ausgegangen, dass für ivacld der Standardanschluss 7136 empfangsbereit ist.

```
svrsslcfg -add_replica  -f <Pfad_zur_Konfigurationsdatei> -h <Hostname>
MSDOS>svrsslcfg -add_replica  -f C:\TAMCSS\TAMCSS.conf -h MyHost.ibm.com
```

Kapitel 3. IBM Clients konfigurieren

Sie müssen zunächst jeden Client mit dem Administratordienstprogramm, einer Komponente von Client Security, konfigurieren, damit Sie dann über den Tivoli Access Manager die Authentifizierungsobjekte für IBM Clients steuern können. Der folgende Abschnitt beschreibt die Voraussetzungen und enthält die Anweisungen für die Konfiguration von IBM Clients.

Voraussetzungen

Stellen Sie sicher, dass die folgende Software in der angegebenen Reihenfolge auf dem IBM Client installiert ist:

1. **Von Microsoft Windows unterstütztes Betriebssystem.** Bei IBM Clients unter Windows XP, Windows 2000 oder Windows NT Workstation 4.0 können Sie über den Tivoli Access Manager die Authentifizierungsbestimmungen steuern.
2. **Client Security ab Version 3.0.** Nach dem Installieren der Software und dem Aktivieren des integrierten IBM Security Chip können Sie mit dem Administratordienstprogramm die Benutzerauthentifizierung konfigurieren und die UVM-Sicherheits-Policy editieren. Ausführliche Anweisungen zur Installation und Verwendung von Client Security sind im *Client Security Installationshandbuch* und im *Client Security Administratorhandbuch* enthalten.

Informationen zur Konfiguration von Tivoli Access Manager angeben

Nach dem Installieren von Tivoli Access Manager auf dem lokalen Client können Sie die Informationen zur Konfiguration von Tivoli Access Manager mit dem Administratordienstprogramm, einer Komponente von Client Security, angeben. Die Informationen zur Konfiguration von Tivoli Access Manager umfassen die folgenden Angaben:

- Vollständigen Pfad für die Konfigurationsdatei auswählen
- Aktualisierungsintervall für lokalen Cache auswählen

Gehen Sie wie folgt vor, um die Informationen zur Konfiguration von Tivoli Access Manager auf dem IBM Client anzugeben:

1. Klicken Sie auf **Start > Einstellungen > Systemsteuerung > Subsystem von IBM Client Security**.
2. Geben Sie das Administratorkennwort ein, und klicken Sie auf **OK**.

   Wenn Sie das Kennwort eingegeben haben, wird das Hauptfenster des Administratordienstprogramms geöffnet.
3. Klicken Sie auf die Schaltfläche **Anwendungsunterstützung und Policies konfigurieren**.

   Die Anzeige "Konfiguration der UVM-Anwendungen und -Policies" wird angezeigt.
4. Aktivieren Sie das Markierungsfeld **Die Windows-Standardanmeldung durch eine gesicherte UVM-Anmeldung ersetzen**.

5. Wählen Sie unter ″Informationen zur Konfiguration von Tivoli Access Manager″ den vollständigen Pfad zur Konfigurationsdatei TAMCSS.conf aus. Beispiel: `C:\TAMCSS\TAMCSS.conf`

   Dieser Bereich wird nur angezeigt, wenn Tivoli Access Manager auf dem Client installiert ist.
6. Klicken Sie auf die Schaltfläche **Anwendungs-Policy...**.
7. Klicken Sie auf die Schaltfläche **Policy bearbeiten**.

   Die Anzeige ″Administratorkennwort eingeben″ erscheint.
8. Geben Sie das Administratorkennwort in das entsprechende Feld ein, und klicken Sie auf **OK**.

   Die Anzeige ″IBM UVM-Policy″ erscheint.
9. Wählen Sie im Dropdown-Menü ″Aktionen″ die Aktionen aus, die über Tivoli Access Manager gesteuert werden sollen.
10. Aktivieren Sie das Markierungsfeld ″Access Manager steuert ausgewähltes Objekt″.
11. Klicken Sie auf die Schaltfläche **Übernehmen**.

    Die Änderung werden bei der nächsten Cache-Aktualisierung wirksam. Wenn Sie möchten, dass die Änderungen sofort wirksam werden, klicken Sie auf die Schaltfläche **Lokalen Cache aktualisieren**.

Lokalen Cache definieren und verwenden

Nach Auswahl der Tivoli Access Manager-Konfigurationsdatei kann das Aktualisierungsintervall für den lokalen Cache festgelegt werden. Auf dem IBM Client wird ein lokales Replikat der von Tivoli Access Manager verwalteten Sicherheits-Policy-Informationen verwaltet. Sie können festlegen, dass der lokale Cache automatisch in einem einem Intervall von Monaten (0 - 12) oder Tagen (0 - 30) aktualisiert wird.

Gehen Sie wie folgt vor, um den lokalen Cache zu definieren oder zu aktualisieren:

1. Klicken Sie auf **Start > Programme > Client Security - Dienstprogramme > Administratordienstprogramm**.
2. Geben Sie das Hardwarekennwort ein, und klicken Sie auf **OK**.

   Das Fenster ″Administratordienstprogramm″ wird angezeigt. Ausführliche Informationen zur Verwendung des Administratordienstprogramms sind im *Client Security Administratorhandbuch* enthalten.
3. Klicken Sie im Administratordienstprogramm auf die Schaltfläche **Anwendungsunterstützung und Policies konfigurieren**.

   Die Anzeige ″Policy-Konfiguration von Client Security ändern″ erscheint.
4. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf **Lokalen Cache aktualisieren**, um den lokalen Cache jetzt zu aktualisieren.
   - Geben Sie den Wert für Monat (0-12) und Tag (0-30) in die entsprechenden Felder ein, und klicken Sie auf **Lokalen Cache aktualisieren**, um die Häufigkeit automatischer Aktualisierungen anzugeben. Der lokale Cache wird aktualisiert und das Ablaufdatum für Dateien im lokalen Cache wird aktualisiert, damit ersichtlich ist, wann die nächste automatische Aktualisierung durchgeführt wird.

Tivoli Access Manager zur Steuerung von IBM Client-Objekten aktivieren

Die UVM-Policy wird durch eine Datei für eine globale Policy gesteuert. Die Datei für eine globale Policy, die sog. UVM-Policy-Datei, enthält Authentifizierungsbestimmungen für Aktionen, die auf dem IBM Client-System ausgeführt werden, wie z. B. am System anmelden, Bildschirmschoner löschen oder E-Mails signieren.

Bearbeiten Sie zunächst mit dem UVM-Policy-Editor die UVM-Policy-Datei, damit Sie den Tivoli Access Manager zur Steuerung der Authentifizierungsobjekte für einen IBM Client verwenden können. Der UVM-Policy-Editor gehört zum Administratordienstprogramm.

Wichtig: Bei der Aktivierung des Tivoli Access Manager zur Steuerung eines Objekts wird die Objektsteuerung dem Tivoli Access Manager-Objektbereich übergeben. Wenn das Objekt dann wieder lokal gesteuert werden soll, müssen Sie Client Security erneut installieren.

Lokale UVM-Policy bearbeiten

Bevor Sie versuchen, die UVM-Policy für den lokalen Client zu bearbeiten, muss mindestens ein Benutzer in UVM registriert sein. Sonst wird eine Fehlernachricht angezeigt, wenn der Policy-Editor versucht, die Datei für die lokale Policy zu öffnen.

Sie bearbeiten eine lokale UVM-Policy, und verwenden sie nur auf dem Client, für den sie bearbeitet wurde. Wurde Client Security im Standardverzeichnis installiert, wird die lokale UVM-Policy im Verzeichnis \Program Files\IBM\Security\UVM_Policy\globalpolicy.gvm gespeichert. Nur ein Benutzer, der UVM hinzugefügt wurde, kann den UVM-Policy-Editor verwenden.

Anmerkung: Wird für UVM-Policy angegeben, dass für ein Authentifizierungsobjekt (wie z. B. die Anmeldung am Betriebssystem) ein Fingerabdruck erforderlich ist, müssen Benutzer, die UVM hinzugefügt sind, ihren Fingerabdruck registrieren lassen, um diese Objekt verwenden zu können.

Führen Sie im Administratordienstprogramm die folgenden Schritte aus, um den UVM-Policy-Editor zu starten:

1. Klicken Sie auf die Schaltfläche **Anwendungsunterstützung und Policies konfigurieren**.

   Die Anzeige ″Policy-Konfiguration von Client Security ändern″ erscheint.
2. Klicken Sie auf die Schaltfläche **Policy bearbeiten**.

   Die Anzeige ″Administratorkennwort eingeben″ erscheint.
3. Geben Sie das Administratorkennwort in das entsprechende Feld ein, und klicken Sie auf **OK**.

   Die Anzeige ″IBM UVM-Policy″ erscheint.
4. Klicken Sie auf der Registerkarte ″Objektauswahl″ auf **Aktion** oder **Objekttyp**, und wählen Sie das Objekt aus, dem Authentifizierungsbestimmungen zugeordnet werden sollen.

   Zu den Beispielen für zulässige Aktionen gehören Systemanmeldung, Entsperren des Systems und E-Mail-Entschlüsselung. Ein Beispiel für den Objekttyp ist ″Digitales Zertifikat anfordern″.

5. Wählen Sie für jedes ausgewählte Objekt **Tivoli Access Manager steuert ausgewähltes Objekt** aus, um den Tivoli Access Manager für das entsprechende Objekt zu aktivieren.

   Wichtig: Wenn Sie den Tivoli Access Manager zur Steuerung eines Objektes auswählen, übergeben Sie die Steuerung dem Tivoli Access Manager-Objektbereich. Wenn dieses Objekt zu einem späteren Zeitpunkt wieder lokal gesteuert werden soll, müssen Sie Client Security erneut installieren.

   Anmerkung: Beim Bearbeiten der UVM-Policy können Sie eine Zusammenfassung der Informationen zur Policy aufrufen, indem Sie auf **Policy-Zusammenfassung** klicken.
6. Klicken Sie auf **Übernehmen**, um Ihre Änderungen zu speichern.
7. Klicken Sie auf **OK**, um den Vorgang zu beenden.

UVM-Policy für ferne Clients bearbeiten und verwenden

Damit die UVM-Policy auf mehreren IBM Clients verwendet werden kann, bearbeiten und speichern Sie die UVM-Policy für einen fernen Client. Anschließend kopieren Sie die UVM-Policy-Datei auf andere IBM Clients. Wenn Sie Client Security im Standardverzeichnis installieren, wird die UVM-Policy-Datei im Verzeichnis ″\Program Files\IBM\Security\UVM_Policy\remote\globalpolicy.gvm″ gespeichert.

Kopieren Sie die folgenden Dateien auf die anderen IBM Clients, auf denen diese UVM-Policy verwendet werden soll:

- \IBM\Security\UVM_Policy\remote\globalpolicy.gvm
- \IBM\Security\UVM_Policy\remote\globalpolicy.gvm.sig

Wurde Client Security im Standardverzeichnis installiert, ist das Stammverzeichnis der oben genannten Pfade \Program Files. Kopieren Sie die beiden Dateien auf den fernen Clients in den Verzeichnispfad \IBM\Security\UVM_Policy\.

Kapitel 4. Fehlerbehebung

Im Folgenden finden Sie Informationen zur Vermeidung, Erkennung und Behebung von Fehlern, die bei der Verwendung von Client Security auftreten können.

Administratorfunktionen

Dieser Abschnitt enthält Informationen für Administratoren zur Konfiguration und zur Verwendung von Client Security.

Administratorkennwort festlegen (ThinkCentre)

Über die Sicherheitseinstellungen im Programm ″Configuration/Setup Utility″ können Administratoren folgende Vorgänge durchführen:

- Das Hardwarekennwort für den integrierten IBM Security Chip ändern
- Den integrierten IBM Security Chip aktivieren oder inaktivieren
- Den Inhalt des integrierten IBM Security Chips löschen

Achtung:

- Löschen oder inaktivieren Sie den integrierten IBM Security Chip nicht bei aktivierter gesicherter UVM-Anmeldung. Andernfalls wird der Inhalt der Festplatte unbrauchbar, und Sie müssen die Festplatte neu formatieren und die gesamte Software neu installieren.

  Um den UVM-Schutz zu inaktivieren, öffnen Sie das Administratordienstprogramm, klicken Sie auf **Anwendungsunterstützung und Policies konfigurieren**, und inaktivieren Sie das Markierungsfeld **Die Windows-Standardanmeldung durch eine gesicherte UVM-Anmeldung ersetzen**. Sie müssen den Computer erneut starten, damit der UVM-Schutz inaktiviert wird.
- Löschen oder inaktivieren Sie den integrierten IBM Security Chip nicht bei aktiviertem UVM-Schutz. Andernfalls haben Sie keinen Zugriff mehr auf das System.
- Wenn Sie den Inhalt des integrierten IBM Security Chips löschen, gehen alle Chiffrierschlüssel und Zertifikate verloren, die auf dem Chip gespeichert sind.

Da auf Ihre Sicherheitseinstellungen über das Programm ″Configuration/Setup Utility″ des Computers zugegriffen werden kann, legen Sie ein Administratorkennwort fest, um zu verhindern, dass diese Einstellungen durch nicht autorisierte Benutzer geändert werden.

Gehen Sie wie folgt vor, um ein Administratorkennwort festzulegen:

1. Fahren Sie das System herunter, und starten Sie es erneut.
2. Drücken Sie während der Eingabeaufforderung des Programms ″Configuration/Setup Utility″ die Taste **F1**.

   Das Hauptmenü des Programms ″Configuration/Setup Utility″ wird geöffnet.
3. Wählen Sie die Option **System Security** aus.
4. Wählen Sie die Option **Administrator Password** aus.
5. Geben Sie das Kennwort ein, und drücken Sie auf der Tastatur die Taste mit dem Abwärtspfeil.
6. Geben Sie das Kennwort erneut ein, und drücken Sie auf der Tastatur die Taste mit dem Abwärtspfeil.

7. Wählen Sie **Change Administrator password** aus, und drücken Sie die Eingabetaste. Drücken Sie danach erneut die Eingabetaste.
8. Drücken Sie die Taste **Esc**, um die Einstellungen zu speichern und das Programm zu verlassen.

Nach dem Festlegen eines Administratorkennworts wird bei jedem Zugriff auf das Programm ″Configuration/Setup Utility″ eine Eingabeaufforderung angezeigt.

Wichtig: Bewahren Sie Ihr Administratorkennwort an einem sicheren Ort auf. Sollten Sie das Administratorkennwort verlieren oder vergessen, können Sie nicht auf das Programm ″Configuration/Setup Utility″ zugreifen und das Kennwort nicht ändern oder löschen, ohne die Computerabdeckung zu entfernen und auf der Systemplatine eine Brücke zu versetzen. Weitere Informationen hierzu finden Sie in der Hardwaredokumentation, die mit Ihrem Computer geliefert wurde.

Administratorkennwort festlegen (ThinkPad)

Mit den Sicherheitseinstellungen im Programm ″IBM BIOS Setup Utility″ können Administratoren folgende Vorgänge durchführen:

- Den integrierten IBM Security Chip aktivieren oder inaktivieren
- Den Inhalt des integrierten IBM Security Chips löschen

Achtung:

- Löschen oder inaktivieren Sie den integrierten IBM Security Chip nicht bei aktivierter gesicherter UVM-Anmeldung. Andernfalls haben Sie keinen Zugriff mehr auf das System.

  Um den UVM-Schutz zu inaktivieren, öffnen Sie das Administratordienstprogramm, klicken Sie auf **Anwendungsunterstützung und Policies konfigurieren**, und inaktivieren Sie das Markierungsfeld **Die Windows-Standardanmeldung durch eine gesicherte UVM-Anmeldung ersetzen**. Sie müssen den Computer erneut starten, damit der UVM-Schutz inaktiviert wird.

  Wenn Sie den Inhalt des integrierten IBM Security Chips löschen, gehen alle Chiffrierschlüssel und Zertifikate verloren, die auf dem Chip gespeichert sind.
- Bei einigen ThinkPad-Modellen ist es vor der Installation oder dem Upgrade von Client Security notwendig, das Administratorkennwort vorübergehend zu inaktivieren.

Nach der Konfiguration von Client Security legen Sie ein Administratorkennwort fest, um nicht berechtigte Benutzer daran zu hindern, diese Einstellungen ändern.

Gehen Sie wie folgt vor, um ein Administratorkennwort festzulegen:

1. Fahren Sie das System herunter, und starten Sie es erneut.
2. Drücken Sie während der Eingabeaufforderung des Programms ″IBM BIOS Setup Utility″ die Taste **F1**.

   Das Hauptmenü des Programms ″IBM BIOS Setup Utility″ wird geöffnet.
3. Wählen Sie die Option **Password** aus.
4. Wählen Sie die Option **Supervisor Password** aus.
5. Geben Sie das Kennwort ein, und drücken Sie die Eingabetaste.
6. Geben Sie das Kennwort erneut ein, und drücken Sie die Eingabetaste.
7. Klicken Sie auf **Continue**.
8. Drücken Sie die Taste F10, um die Einstellungen zu speichern und das Programm zu beenden.

Nach dem Festlegen eines Administratorkennworts wird bei jedem Zugriff auf das Programm ″IBM BIOS Setup Utility″ eine Eingabeaufforderung angezeigt.

Wichtig: Bewahren Sie Ihr Administratorkennwort an einem sicheren Ort auf. Sollten Sie das Administratorkennwort verlieren oder vergessen, können Sie nicht auf das Programm ″IBM BIOS Setup Utility″ zugreifen und das Kennwort nicht ändern oder löschen. Weitere Informationen hierzu finden Sie in der Hardwaredokumentation, die mit Ihrem Computer geliefert wurde.

Hardwarekennwort schützen

Sie können ein Kennwort für den IBM Security Chip festlegen, um den integrierten IBM Security Chip für einen Client zu aktivieren. Nachdem Sie das Kennwort für den IBM Security Chip festgelegt haben, ist der Zugriff auf das Administratordienstprogramm durch dieses Kennwort geschützt. Sie müssen das Kennwort für den IBM Security Chip vor unberechtigtem Zugriff schützen, damit nicht berechtigte Benutzer die Einstellungen im Administratordienstprogramm nicht ändern können.

Inhalt des integrierten IBM Security Chips löschen (ThinkCentre)

Wenn Sie alle Chiffrierschlüssel für Benutzer aus dem integrierten IBM Security Chip sowie das Hardwarekennwort für den Chip löschen möchten, müssen Sie den Inhalt des Chips löschen. Lesen Sie die nachfolgend unter ″Achtung″ aufgeführten Informationen, bevor Sie den Inhalt des integrierten IBM Security Chips löschen.

Achtung:

- Löschen oder inaktivieren Sie den integrierten IBM Security Chip nicht bei aktiviertem UVM-Schutz. Andernfalls haben Sie keinen Zugriff mehr auf das System.

  Um den UVM-Schutz zu inaktivieren, öffnen Sie das Administratordienstprogramm, klicken Sie auf **Anwendungsunterstützung und Policies konfigurieren**, und inaktivieren Sie das Markierungsfeld **Die Windows-Standardanmeldung durch eine gesicherte UVM-Anmeldung ersetzen**. Sie müssen den Computer erneut starten, damit der UVM-Schutz inaktiviert wird.
- Wenn Sie den Inhalt des integrierten IBM Security Chips löschen, gehen alle Chiffrierschlüssel und Zertifikate verloren, die auf dem Chip gespeichert sind.

Gehen Sie wie folgt vor, um den Inhalt des integrierten IBM Security Chips zu löschen:

1. Fahren Sie das System herunter, und starten Sie es erneut.
2. Drücken Sie während der Eingabeaufforderung des Programms ″Configuration/Setup Utility″ die Taste **F1**.

   Das Hauptmenü des Programms ″Configuration/Setup Utility″ wird geöffnet.
3. Wählen Sie die Option **Security** aus.
4. Wählen Sie **IBM TCPA Feature Setup** aus.
5. Wählen Sie **Clear IBM TCPA Security Feature** aus.
6. Wählen Sie **Yes** aus.
7. Drücken Sie die Taste ″Esc″, um fortzufahren.
8. Drücken Sie Taste ″Esc″, um das Programm zu verlassen und die Einstellungen zu speichern.

Inhalt des integrierten IBM Security Chips löschen (ThinkPad)

Wenn Sie alle Chiffrierschlüssel für Benutzer aus dem integrierten IBM Security Chip und das Hardwarekennwort für den Chip löschen möchten, müssen Sie den Inhalt des Chips löschen. Lesen Sie die nachfolgend unter ″Achtung″ aufgeführten Informationen, bevor Sie den Inhalt des integrierten IBM Security Chips löschen.

Achtung:

- Löschen oder inaktivieren Sie bei aktiviertem UVM-Schutz den integrierten IBM Security Chip nicht. Andernfalls wird der Inhalt der Festplatte unbrauchbar, und Sie müssen die Festplatte neu formatieren und die gesamte Software neu installieren.

  Um den UVM-Schutz zu inaktivieren, öffnen Sie das Administratordienstprogramm, klicken Sie auf **Anwendungsunterstützung und Policies konfigurieren**, und inaktivieren Sie das Markierungsfeld **Die Windows-Standardanmeldung durch eine gesicherte UVM-Anmeldung ersetzen**. Sie müssen den Computer erneut starten, damit der UVM-Schutz inaktiviert wird.
- Wenn Sie den Inhalt des integrierten IBM Security Chips löschen, gehen alle Chiffrierschlüssel und Zertifikate verloren, die auf dem Chip gespeichert sind.

Gehen Sie wie folgt vor, um den Inhalt des integrierten IBM Security Chips zu löschen:

1. Fahren Sie das System herunter, und starten Sie es erneut.
2. Drücken Sie während der Eingabeaufforderung des Programms ″IBM BIOS Setup Utility″ die Taste ″Fn″.

   Anmerkung: Auf einigen ThinkPad-Modellen müssen Sie möglicherweise beim Einschalten die Taste F1 drücken, um auf das Programm ″IBM BIOS Setup Utility″ zuzugreifen. Weitere Informationen hierzu finden Sie in der Hilfenachricht des Programms ″IBM BIOS Setup Utility″.

   Das Hauptmenü des Programms ″IBM BIOS Setup Utility″ wird geöffnet.
3. Wählen Sie **Config** aus.
4. Wählen Sie **IBM Security Chip** aus.
5. Wählen Sie **Clear IBM Security Chip** aus.
6. Wählen Sie **Yes** aus.
7. Drücken Sie die Eingabetaste, um fortzufahren.
8. Drücken Sie die Taste F10, um die Einstellungen zu speichern und das Programm zu beenden.

Administratordienstprogramm

Der folgende Abschnitt enthält Informationen, die Sie bei der Verwendung des Administratordienstprogramms beachten müssen.

Benutzer löschen

Wenn Sie einen Benutzer löschen, wird der Benutzername in der Benutzerliste des Administratordienstprogramms gelöscht.

Keinen Zugriff auf ausgewählte Objekte mit der Tivoli Access Manager-Steuerung zulassen

Das Markierungsfeld **Keinen Zugriff auf ausgewähltes Objekt zulassen** ist nicht inaktiviert, wenn die Tivoli Access Manager-Steuerung ausgewählt wurde. Wenn Sie im UVM-Policy-Editor die Option **Access Manager steuert ausgewähltes Objekt** auswählen, um ein Authentifizierungsobjekt über Tivoli Access Manager zu steuern, wird das Markierungsfeld **Keinen Zugriff auf ausgewähltes Objekt zulassen** nicht inaktiviert. Auch wenn das Markierungsfeld **Keinen Zugriff auf ausgewähltes Objekt zulassen** weiterhin aktiviert ist, kann die Tivoli Access Manager-Steuerung nicht über dieses Markierungsfeld außer Kraft gesetzt werden.

Bekannte Einschränkungen

Dieser Abschnitt enthält Informationen zu bekannten Einschränkungen in Bezug auf Client Security.

Client Security mit Windows-Betriebssystemen einsetzen

Alle Windows-Betriebssysteme weisen die folgende bekannte Einschränkung auf: Wenn ein in UVM registrierter Clientbenutzer seinen Windows-Benutzernamen ändert, geht die gesamte Funktionalität von Client Security verloren. Der Benutzer muss den neuen Benutzernamen erneut in UVM registrieren und alle neuen Berechtigungsnachweise anfordern.

Windows XP-Betriebssysteme weisen die folgende bekannte Einschränkung auf: In UVM registrierte Benutzer, deren Windows-Benutzername zuvor geändert wurde, werden von UVM nicht erkannt. UVM verweist auf den früheren Benutzernamen, während Windows nur den neuen Benutzernamen erkennt. Diese Einschränkung gilt selbst dann, wenn der Windows-Benutzername vor der Installation von Client Security geändert wurde.

Client Security mit Netscape-Anwendungen einsetzen

Netscape wird nach einem Berechtigungsfehler geöffnet: Wenn das Fenster ″UVM-Verschlüsselungstext″ geöffnet wird, müssen Sie den UVM-Verschlüsselungstext eingeben und auf **OK** klicken, bevor Sie fortfahren können. Wenn Sie einen falschen UVM-Verschlüsselungstext eingeben (oder bei einer Scannerabtastung von Fingerabdrücken einen falschen Fingerabdruck liefern), wird eine Fehlernachricht angezeigt. Wenn Sie auf **OK** klicken, wird Netscape geöffnet, Sie können aber das vom integrierten IBM Security Chip generierte digitale Zertifikat nicht verwenden. Sie müssen Netscape verlassen, erneut aufrufen und den richtigen UVM-Verschlüsselungstext eingeben, bevor Sie das Zertifikat für den integrierten IBM Security Chip verwenden können.

Algorithmen werden nicht angezeigt: Beim Anzeigen des Moduls in Netscape ist keiner der vom PKCS #11-Modul des integrierten IBM Security Chips unterstützten Hashverfahren-Algorithmen ausgewählt. Die folgenden Algorithmen werden vom PKCS #11-Modul des integrierten IBM Security Chips unterstützt, jedoch nicht als unterstützt erkannt, wenn sie in Netscape angezeigt werden:

- SHA-1
- MD5

Zertifikat des integrierten IBM Security Chips und Verschlüsselungsalgorithmen

Im Folgenden finden Sie Informationen zu Verschlüsselungsalgorithmen, die Sie mit dem Zertifikat des integrierten IBM Security Chips verwenden können. Aktuelle Informationen zu Verschlüsselungsalgorithmen für die jeweilige E-Mail-Anwendung erhalten Sie von Microsoft oder Netscape.

Beim Senden von E-Mails von einem Outlook Express-Client (128 Bit) an einen anderen Outlook Express-Client (128 Bit): Wenn Sie Outlook Express mit der 128-Bit-Version von Internet Explorer 4.0 oder 5.0 verwenden, um verschlüsselte E-Mails an andere Clients mit Outlook Express (128 Bit) zu senden, können mit dem Zertifikat des integrierten IBM Security Chips verschlüsselte E-Mails nur mit dem 3DES-Algorithmus verschlüsselt werden.

Beim Senden von E-Mails zwischen einem Outlook Express-Client (128 Bit) und einem Netscape-Client: Eine Verschlüsselungsanforderung gemäß RC2(40), RC2(64) oder RC2(128) von einem Netscape-Client an einen Outlook Express-Client (128 Bit) wird an den Netscape-Client immer mit dem RC2(40)-Algorithmus zurückgesendet.

Möglicherweise stehen einige Algorithmen im Outlook Express-Client (128 Bit) nicht zur Auswahl: Je nachdem, wie die Version von Outlook Express (128 Bit) konfiguriert oder aktualisiert wurde, sind möglicherweise einige RC2-Algorithmen und andere Algorithmen für die Verwendung mit dem Zertifikat des integrierten IBM Security Chips nicht verfügbar. Aktuelle Informationen zu den Verschlüsselungsalgorithmen, die mit den verschiedenen Versionen von Outlook Express verwendet werden, erhalten Sie von Microsoft.

UVM-Schutz für eine Lotus Notes-Benutzer-ID verwenden

Der UVM-Schutz funktioniert nicht, wenn Sie innerhalb einer Notes-Sitzung die Benutzer-ID wechseln: Sie können den UVM-Schutz nur für die aktuelle Benutzer-ID einer Notes-Sitzung konfigurieren. Gehen Sie wie folgt vor, um von einer Benutzer-ID, für die UVM-Schutz aktiviert wurde, zu einer anderen Benutzer-ID zu wechseln:

1. Verlassen Sie Lotus Notes.
2. Inaktivieren Sie den UVM-Schutz für die aktuelle Benutzer-ID.
3. Rufen Sie Lotus Notes auf, und wechseln Sie die Benutzer-ID. Weitere Informationen zum Wechseln von Benutzer-IDs finden Sie in der Dokumentation zu Lotus Notes.

   Wenn Sie den UVM-Schutz für die Benutzer-ID, zu der Sie gewechselt haben, konfigurieren möchten, fahren Sie mit Schritt 4 fort.
4. Rufen Sie das von Client Security bereitgestellte Tool zur Lotus Notes-Konfiguration auf, und konfigurieren Sie den UVM-Schutz.

Einschränkungen für das Benutzerkonfigurationsprogramm

Unter Windows XP gibt es für einen Clientbenutzer unter bestimmten Umständen Zugriffseinschränkungen für die verfügbaren Funktionen.

Windows XP Professional

Unter Windows XP Professional können die Einschränkungen für Clientbenutzer in den folgenden Situationen auftreten:

- Client Security ist auf einer Partition installiert, die später in das NTFS-Format konvertiert wird.
- Der Windows-Ordner befindet sich auf einer Partition, die später in das NTFS-Format konvertiert wird.
- Der Archivordner befindet sich auf einer Partition, die später in das NTFS-Format konvertiert wird.

In den vorgenannten Fällen können Benutzer von Windows XP Professional mit eingeschränkter Berechtigung möglicherweise folgende Tasks im Benutzerkonfigurationsprogramm nicht ausführen:

- Den UVM-Verschlüsselungstext ändern
- Das mit UVM registrierte Windows-Kennwort aktualisieren
- Das Schlüsselarchiv aktualisieren

Diese Einschränkungen gelten nicht mehr, nachdem ein Administrator das Administratordienstprogramm gestartet und beendet hat.

Windows XP Home

Benutzer von Windows XP Home mit eingeschränkter Berechtigung können in den folgenden Fällen das Benutzerkonfigurationsprogramm nicht verwenden:

- Client Security ist auf einer Partition im NTFS-Format installiert.
- Der Windows-Ordner befindet sich auf einer Partition im NTFS-Format.
- Der Archivordner befindet sich auf einer Partition im NTFS-Format.

Fehlernachrichten

Fehlernachrichten für Client Security werden in Ereignisprotokoll geschrieben: Client Security verwendet einen Einheitentreiber, der möglicherweise Fehlernachrichten in das Ereignisprotokoll schreibt. Die Fehler, auf denen diese Nachrichten basieren, wirken sich auf den normalen Betrieb des Computers nicht aus.

UVM ruft Fehlernachrichten auf, die vom zugeordneten Programm generiert werden, wenn für ein Authifizierungsobjekt der Zugriff verweigert wird: Wenn in der UVM-Policy die Verweigerung des Zugriffs für ein Authentifizierungsobjekt, z. B. für die E-Mail-Verschlüsselung festgelegt ist, variiert die Nachricht über den verweigerten Zugriff je nach verwendeter Software. Eine Fehlernachricht von Outlook Express über die Verweigerung des Zugriffs auf ein Authentifizierungsobjekt unterscheidet sich somit von einer Netscape-Fehlernachricht über verweigerten Zugriff.

Fehlerbehebungstabellen

Im folgenden Abschnitt finden Sie Tabellen, die Ihnen bei der Behebung von Fehlern in Verbindung mit Client Security weiterhelfen können.

Fehlerbehebungsinformationen zur Installation

Im folgenden Abschnitt finden Sie Informationen, die Ihnen bei der Behebung von Fehlern bei der Installation von Client Security weiterhelfen können.

Fehlersymptom	Mögliche Lösung
Während der Softwareinstallation wird eine Fehlernachricht angezeigt.	**Maßnahme**
Bei der Softwareinstallation werden Sie in einer Nachricht gefragt, ob Sie die ausgewählte Anwendung und alle zugehörigen Komponenten entfernen möchten.	Klicken Sie auf **OK**, um das Fenster zu verlassen. Beginnen Sie erneut mit dem Installationsprozess, um die neue Version von Client Security zu installieren.
Während der Installation wird eine Nachricht angezeigt, die besagt, dass bereits eine vorherige Version von Client Security installiert ist.	Klicken Sie auf **OK**, um das Fenster zu verlassen. Gehen Sie wie folgt vor: 1. Deinstallieren Sie die Software. 2. Installieren Sie die Software erneut. **Anmerkung:** Wenn Sie dasselbe Hardwarekennwort zum Schutz des integrierten IBM Security Chips verwenden möchten, müssen Sie den Inhalt des Chips nicht löschen und kein neues Kennwort festlegen.
Der Installationszugriff wird verweigert, da das Hardwarekennwort unbekannt ist	**Maßnahme**
Wenn Sie die Software auf einem IBM Client mit aktiviertem integrierten IBM Security Chip installieren, ist das Hardwarekennwort für den integrierten IBM Security Chip unbekannt.	Löschen Sie den Inhalt des Chips, um mit der Installation fortzufahren.
Die Datei ″setup.exe″ reagiert nicht ordnungsgemäß (CSS Version 4.0x)	**Maßnahme**
Wenn Sie alle Dateien aus ″csec4_0.exe″ in ein gemeinsames Verzeichnis extrahieren, funktioniert die Datei ″setup.exe″ nicht ordnungsgemäß.	Führen Sie die Datei ″smbus.exe″ aus, um den SMBus-Einheitentreiber zu installieren, und führen Sie anschließend die Datei ″csec4_0.exe″ aus, um den Softwarecode von Client Security zu installieren.

Fehlerbehebungsinformationen zum Administratordienstprogramm

Im folgenden Abschnitt finden Sie Informationen, die Ihnen bei der Behebung von Fehlern bei der Verwendung des Administratordienstprogramms weiterhelfen können.

Fehlersymptom	Mögliche Lösung
Policy für UVM-Verschlüsselungstext nicht erzwungen	**Maßnahme**
Das Markierungsfeld **Mehr als 2 wiederkehrende Zeichen nicht zulassen** funktioniert nicht in IBM Client Security Version 5.0	Dies ist eine bekannte Einschränkung bei IBM Client Security Version 5.0.
Die Schaltfläche "Weiter" ist nicht verfügbar, nachdem Sie im Administratordienstprogramm den UVM-Verschlüsselungstext eingegeben und bestätigt haben.	**Maßnahme**
Wenn Sie neue Benutzer in UVM aufnehmen, ist die Schaltfläche **Weiter** möglicherweise nicht mehr verfügbar, nachdem Sie Ihren UVM-Verschlüsselungstext im Administratordienstprogramm eingegeben und bestätigt haben.	Klicken Sie in der Windows-Taskleiste auf **Informationen**, und fahren Sie mit dem Vorgang fort.
Beim Versuch, eine lokale UVM-Policy zu bearbeiten, wird eine Fehlernachricht angezeigt.	**Maßnahme**
Beim Bearbeiten der lokalen UVM-Policy wird möglicherweise eine Fehlernachricht angezeigt, wenn in UVM keine Benutzer registriert sind.	Fügen Sie in UVM einen Benutzer hinzu, bevor Sie versuchen, die Policy-Datei zu bearbeiten.
Beim Ändern des öffentlichen Schlüssels für Administratoren wird eine Fehlernachricht angezeigt.	**Maßnahme**
Wenn Sie den Inhalt des integrierten Security Chips löschen und anschließend das Schlüsselarchiv wiederherstellen, wird bei der Änderung des öffentlichen Schlüssels für Administratoren möglicherweise eine Fehlernachricht angezeigt.	Fügen Sie in UVM die Benutzer hinzu, und fordern Sie ggf. neue Zertifikate an.
Beim Versuch, einen UVM-Verschlüsselungstext wiederherzustellen, wird eine Fehlernachricht angezeigt.	**Maßnahme**
Wenn Sie einen öffentlichen Schlüssel für Administratoren ändern und anschließend versuchen, einen UVM-Verschlüsselungstext für einen Benutzer wiederherzustellen, wird möglicherweise eine Fehlernachricht angezeigt.	Führen Sie einen der folgenden Schritte aus: • Sollte für den Benutzer der UVM-Verschlüsselungstext nicht benötigt werden, ist keine Maßnahme erforderlich. • Wenn der UVM-Verschlüsselungstext für den Benutzer erforderlich ist, müssen Sie ihn in UVM aufnehmen und ggf. neue Zertifikate anfordern.

Fehlersymptom	Mögliche Lösung
Beim Versuch, die UVM-Policy-Datei zu speichern, wird eine Fehlernachricht angezeigt.	**Maßnahme**
Wenn Sie versuchen, eine UVM-Policy-Datei (globalpolicy.gvm) durch Klicken auf **Übernehmen** oder **Speichern** zu speichern, wird eine Fehlernachricht angezeigt.	Schließen Sie die Fehlernachricht, bearbeiten Sie die UVM-Policy-Datei erneut, und speichern Sie die Datei.
Beim Versuch, den UVM-Policy-Editor zu öffnen, wird eine Fehlernachricht angezeigt.	**Maßnahme**
Wenn der aktuelle Benutzer, der am Betriebssystem angemeldet ist, nicht in UVM aufgenommen wurde, wird der UVM-Policy-Editor nicht geöffnet.	Nehmen Sie den Benutzer in UVM auf, und öffnen Sie den UVM-Policy-Editor.
Bei der Verwendung des Administratordienstprogramms wird eine Fehlernachricht angezeigt.	**Maßnahme**
Während Sie das Administratordienstprogramm verwenden, wird möglicherweise die folgende Fehlernachricht angezeigt: Beim Versuch, auf den Client Security Chip zuzugreifen, ist ein Puffer-E/A-Fehler aufgetreten. Der Fehler kann möglicherweise durch einen Warmstart behoben werden.	Schließen Sie die Fehlernachricht, und starten Sie den Computer erneut.
Beim Ändern des Kennworts für den Security Chip wird eine Nachricht über die Inaktivierung des Chips angezeigt.	**Maßnahme**
Wenn Sie versuchen, das Kennwort für den IBM Security Chip zu ändern, und nach der Eingabe des Bestätigungskennworts die Eingabetaste oder die Tabulatortaste zusammen mit der Eingabetaste drücken, wird die Schaltfläche ″Chip inaktivieren″ aktiviert, und es wird eine Bestätigungsnachricht für das Inaktivieren des Chips angezeigt.	Gehen Sie wie folgt vor: 1. Schließen Sie das Bestätigungsfenster für die Inaktivierung des Chips. 2. Geben Sie zum Ändern des Kennworts für den IBM Security Chip das neue Kennwort ein, geben Sie das Bestätigungskennwort ein, und klicken Sie anschließend auf **Ändern**. Drücken Sie, nachdem Sie das Bestätigungskennwort eingegeben haben, nicht die Eingabetaste oder die Tabulatortaste zusammen mit der Eingabetaste.

Fehlerbehebungsinformationen zum Benutzerkonfigurationsprogramm

Die folgenden Informationen zur Fehlerbehebung können hilfreich sein, wenn bei der Verwendung des Benutzerkonfigurationsprogramms Fehler auftreten.

Fehlersymptom	Mögliche Lösung
Benutzer mit eingeschränkter Berechtigung können gewisse Funktionen des Benutzerkonfigurationsprogramms unter Windows XP Professional nicht ausführen	**Maßnahme**
Benutzer von Windows XP Professional mit eingeschränkter Berechtigung können möglicherweise folgende Tasks im Benutzerkonfigurationsprogramm nicht ausführen: • Den UVM-Verschlüsselungstext ändern • Das mit UVM registrierte Windows-Kennwort aktualisieren • Das Schlüsselarchiv aktualisieren	Diese Einschränkungen gelten nicht mehr, nachdem ein Administrator das Administratordienstprogramm gestartet und beendet hat.
Benutzer mit eingeschränkter Berechtigung können das Benutzerkonfigurationsprogramm unter Windows XP Home nicht ausführen	**Maßnahme**
Benutzer von Windows XP Home mit eingeschränkter Berechtigung können in den folgenden Fällen das Benutzerkonfigurationsprogramm nicht verwenden: • Client Security ist auf einer Partition im NTFS-Format installiert. • Der Windows-Ordner befindet sich auf einer Partition im NTFS-Format. • Der Archivordner befindet sich auf einer Partition im NTFS-Format.	Dies ist eine bekannte Einschränkung unter Windows XP Home. Für dieses Problem gibt es keine Lösung.

Fehlerbehebungsinformationen zum ThinkPad

Im folgenden Abschnitt finden Sie Informationen, die Ihnen bei der Behebung von Fehlern bei der Verwendung von Client Security auf ThinkPads weiterhelfen können.

Fehlersymptom	Mögliche Lösung
Beim Versuch, eine Administratorfunktion von Client Security aufzurufen, wird eine Fehlernachricht angezeigt.	**Maßnahme**
Nach dem Versuch, eine Administratorfunktion von Client Security aufzurufen, wird eine Fehlernachricht mit folgendem Wortlaut angezeigt: ″FEHLER 0197: Ungültige ferne Änderungsanforderung. Drücken Sie <F1>, um Setup aufzurufen.″	Das ThinkPad-Administratorkennwort muss inaktiviert sein, damit Sie bestimmte Administratorfunktionen von Client Security ausführen können. Gehen Sie wie folgt vor, um das Administratorkennwort zu inaktivieren: 1. Rufen Sie mit ″F1″ das Programm ″IBM BIOS Setup Utility″ auf. 2. Geben Sie das aktuelle Administratorkennwort ein. 3. Geben Sie ein leeres neues Administratorkennwort ein, und bestätigen Sie das leere Kennwort. 4. Drücken Sie die Eingabetaste. 5. Drücken Sie die Taste F10, um die Einstellungen zu speichern und das Programm zu beenden.
Ein anderer UVM-Sensor für Fingerabdrücke funktioniert nicht ordnungsgemäß.	**Maßnahme**
Der IBM ThinkPad unterstützt den Wechsel zwischen mehreren UVM-Sensoren für Fingerabdrücke nicht.	Wechseln Sie die Modelle der Sensoren für Fingerabdrücke nicht. Verwenden Sie bei der Arbeit von einem fernen Standort aus stets das gleiche Modell wie bei der Arbeit an einer Andockstation.

Fehlerbehebungsinformationen zu Microsoft-Anwendungen und -Betriebssystemen

Die folgenden Fehlerbehebungstabellen enthalten Informationen zur Fehlerbehebung bei der Verwendung von Client Security mit Microsoft-Anwendungen oder -Betriebssystemen.

Fehlersymptom	Mögliche Lösung
Bildschirmschoner wird nur auf lokaler Anzeige angezeigt	**Maßnahme**
Bei Verwendung des erweiterten Windows-Desktop wird der Client Security-Bildschirmschoner nur auf der lokalen Anzeige angezeigt, obwohl der Zugriff auf das System und die Tastatur geschützt wird.	Wenn sensible Informationen angezeigt werden, verkleinern Sie die Fenster auf Ihrem erweiterten Desktop auf Symbolgröße, bevor Sie den Client Security-Bildschirmschoner aufrufen.
Windows Media Player-Dateien werden verschlüsselt, statt unter Windows XP wiedergegeben zu werden.	**Maßnahme**

Fehlersymptom	Mögliche Lösung
Wenn Sie unter Windows XP einen Ordner öffnen und auf **Alles wiedergeben** klicken, wird der Dateiinhalt verschlüsselt, statt vom Windows Media Player wiedergegeben zu werden.	Gehen Sie wie folgt vor, um die Wiedergabe von Dateien mit dem Windows Media Player zu aktivieren: 1. Starten Sie den Windows Media Player. 2. Wählen Sie alle Dateien im entsprechenden Ordner aus. 3. Ziehen Sie die Dateien in den Bereich ″Wiedergabeliste″ von Windows Media Player.
Client Security funktioniert für einen in UVM registrierten Benutzer nicht ordnungsgemäß.	**Maßnahme**
Der registrierte Clientbenutzer hat möglicherweise seinen Windows-Benutzernamen geändert. Wenn dies zutrifft, geht die gesamte Funktionalität von Client Security verloren.	Registrieren Sie den neuen Benutzernamen in UVM erneut, und fordern Sie alle neuen Berechtigungsnachweise an.
Anmerkung: Unter Windows XP werden in UVM registrierte Benutzer, deren Windows-Benutzername zuvor geändert wurde, von UVM nicht erkannt. Diese Einschränkung gilt selbst dann, wenn der Windows-Benutzername vor der Installation von Client Security geändert wurde.	
Fehler beim Lesen verschlüsselter E-Mails mit Outlook Express	**Maßnahme**
Verschlüsselte E-Mails können nicht entschlüsselt werden, da sich die Verschlüsselungsgrade der Webbrowser, die vom Sender und vom Empfänger verwendet werden, unterscheiden. **Anmerkung:** Wenn Sie Browser mit 128-Bit-Verschlüsselung mit Client Security verwenden möchten, muss der integrierte IBM Security Chip 256-Bit-Verschlüsselung unterstützen. Wenn der integrierte IBM Security Chip 56-Bit-Verschlüsselung unterstützt, müssen Sie einen 40-Bit-Webbrowser verwenden. Der Verschlüsselungsgrad von Client Security ist im Administratordienstprogramm angegeben.	Überprüfen Sie Folgendes: 1. Der Verschlüsselungsgrad des Webbrowsers beim Sender muss mit dem Verschlüsselungsgrad des Webbrowsers des Empfängers kompatibel sein. 2. Der Verschlüsselungsgrad des Webbrowsers muss mit dem Verschlüsselungsgrad der Firmware von Client Security kompatibel sein.
Fehler bei der Verwendung eines Zertifikats von einer Adresse, der mehrere Zertifikate zugeordnet sind	**Maßnahme**
Outlook Express kann mehrere Zertifikate zu einer einzigen E-Mail-Adresse auflisten, und einige dieser Zertifikate können ungültig werden. Ein Zertifikat wird ungültig, wenn der dem Zertifikat zugeordnete private Schlüssel auf dem integrierten IBM Security Chip des Sendercomputers, auf dem das Zertifikat generiert wurde, nicht mehr vorhanden ist.	Bitten Sie den Empfänger, sein digitales Zertifikat erneut zu senden; wählen Sie anschließend dieses Zertifikat im Adressbuch von Outlook Express aus.

Fehlersymptom	Mögliche Lösung
Beim Versuch, eine E-Mail digital zu signieren, wird eine Fehlernachricht angezeigt.	**Maßnahme**
Wenn der Verfasser einer E-Mail versucht, eine E-Mail digital zu signieren, jedoch seinem E-Mail-Account noch kein Zertifikat zugeordnet ist, wird eine Fehlernachricht angezeigt.	Verwenden Sie die Sicherheitseinstellungen in Outlook Express, um ein Zertifikat anzugeben, das dem Benutzeraccount zugeordnet werden soll. Weitere Informationen hierzu finden Sie in der Dokumentation zu Outlook Express.
Outlook Express (128 Bit) verschlüsselt E-Mails nur mit dem 3DES-Algorithmus.	**Maßnahme**
Beim Senden verschlüsselter E-Mails zwischen Clients, die Outlook Express mit der 128-Bit-Version von Internet Explorer 4.0 oder 5.0 verwenden, kann nur der 3DES-Algorithmus verwendet werden.	Wenn Sie Browser mit 128-Bit-Verschlüsselung mit Client Security verwenden möchten, muss der integrierte IBM Security Chip 256-Bit-Verschlüsselung unterstützen. Wenn der integrierte IBM Security Chip 56-Bit-Verschlüsselung unterstützt, müssen Sie einen 40-Bit-Webbrowser verwenden. Der Verschlüsselungsgrad von Client Security ist im Administratordienstprogramm angegeben. Aktuelle Informationen zu den Verschlüsselungsalgorithmen, die mit Outlook Express verwendet werden, erhalten Sie bei Microsoft.
Outlook Express-Clients senden E-Mails mit einem anderen Algorithmus zurück.	**Maßnahme**
Eine mit dem RC2(40)-, RC2(64)- oder RC2(128)-Algorithmus verschlüsselte E-Mail wird von einem Client mit Netscape Messenger an einen Client mit Outlook Express (128 Bit) gesendet. Eine vom Outlook Express-Client zurückgesendete E-Mail wird mit dem Algorithmus RC2(40) verschlüsselt.	Es ist keine Maßnahme erforderlich. Eine Verschlüsselungsanforderung gemäß RC2(40), RC2(64) oder RC2(128) von einem Netscape-Client an einen Outlook Express-Client (128 Bit) wird an den Netscape-Client immer mit dem RC2(40)-Algorithmus zurückgesendet. Aktuelle Informationen zu den Verschlüsselungsalgorithmen, die mit den verschiedenen Versionen von Outlook Express verwendet werden, erhalten Sie von Microsoft.
Bei der Verwendung eines Zertifikats in Outlook Express wird nach dem Ausfall eines Festplattenlaufwerks eine Fehlernachricht angezeigt.	**Maßnahme**
Zertifikate können im Administratordienstprogramm mit der Wiederherstellungsfunktion für Schlüssel wiederhergestellt werden. Möglicherweise sind einige Zertifikate, wie z. B. die kostenfreien Zertifikate von VeriSign, nach einer Schlüsselwiederherstellung nicht wiederhergestellt.	Führen Sie nach der Wiederherstellung der Schlüssel einen der folgenden Schritte aus: • Fordern Sie neue Zertifikate an. • Registrieren Sie die Zertifizierungsinstanz erneut in Outlook Express.

Fehlersymptom	Mögliche Lösung
Outlook Express aktualisiert den dem Zertifikat zugeordneten Verschlüsselungsgrad nicht.	**Maßnahme**
Wenn ein Sender den Verschlüsselungsgrad in Netscape auswählt und eine signierte E-Mail an einen Outlook Express-Client mit Internet Explorer 4.0 (128 Bit) sendet, stimmt möglicherweise der Verschlüsselungsgrad der zurückgesendeten E-Mail nicht überein.	Löschen Sie das zugeordnete Zertifikat aus dem Adressbuch von Outlook Express. Öffnen Sie die signierte E-Mail erneut, und fügen Sie dem Adressbuch von Outlook Express das Zertifikat hinzu.
In Outlook Express wird eine Nachricht über Entschlüsselungsfehler angezeigt.	**Maßnahme**
Sie können in Outlook Express eine Nachricht öffnen, indem Sie doppelt darauf klicken. Wenn Sie zu schnell auf eine verschlüsselte Nachricht klicken, wird in einigen Fällen eine Nachricht über Entschlüsselungsfehler angezeigt.	Schließen Sie die Nachricht, und öffnen Sie die verschlüsselte E-Mail erneut.
Darüber hinaus wird möglicherweise in der Voranzeige eine Fehlernachricht angezeigt, wenn Sie eine verschlüsselte Nachricht auswählen.	Wenn in der Voranzeige eine Fehlernachricht angezeigt wird, ist keine Maßnahme erforderlich.
Wenn Sie bei verschlüsselten E-Mails zwei Mal auf die Schaltfläche ″Senden″ klicken, wird eine Fehlernachricht angezeigt	**Maßnahme**
Wenn Sie in Outlook Express zweimal auf die Schaltfläche zum Senden klicken, um eine verschlüsselte E-Mail zu senden, wird eine Fehlernachricht darüber angezeigt, dass die Nachricht nicht gesendet werden konnte.	Schließen Sie die Fehlernachricht, und klicken Sie einmal auf die Schaltfläche **Senden**.
Beim Anfordern eines Zertifikats wird eine Fehlernachricht angezeigt.	**Maßnahme**
Bei Verwendung von Internet Explorer erhalten Sie möglicherweise eine Fehlernachricht, wenn Sie ein Zertifikat anfordern, das das CSP-Modul des integrierten IBM Security Chips verwendet.	Fordern Sie das digitale Zertifikat erneut an.

Fehlerbehebungsinformationen zu Netscape-Anwendungen

Die folgenden Fehlerbehebungstabellen enthalten Informationen zur Fehlerbehebung bei der Verwendung von Client Security mit Netscape-Anwendungen.

Fehlersymptom	Mögliche Lösung
Fehler beim Lesen verschlüsselter E-Mails	**Maßnahme**
Verschlüsselte E-Mails können nicht entschlüsselt werden, da sich die Verschlüsselungsgrade der Webbrowser, die vom Sender und vom Empfänger verwendet werden, unterscheiden. **Anmerkung:** Wenn Sie Browser mit 128-Bit-Verschlüsselung mit Client Security verwenden möchten, muss der integrierte IBM Security Chip 256-Bit-Verschlüsselung unterstützen. Wenn der integrierte IBM Security Chip 256-Bit-Verschlüsselung unterstützt, müssen Sie einen 40-Bit-Webbrowser verwenden. Der Verschlüsselungsgrad von Client Security ist im Administratordienstprogramm angegeben.	Überprüfen Sie Folgendes: 1. Der Verschlüsselungsgrad des vom Sender verwendeten Webbrowsers ist mit dem Verschlüsselungsgrad des vom Empfänger verwendeten Webbrowsers kompatibel. 2. Der Verschlüsselungsgrad des Webbrowsers ist mit dem Verschlüsselungsgrad kompatibel, der von der Firmware von Client Security bereitgestellt wird.
Beim Versuch, eine E-Mail digital zu signieren, wird eine Fehlernachricht angezeigt.	**Maßnahme**
Wenn das Zertifikat des integrierten IBM Security Chips in Netscape Messenger nicht ausgewählt wurde und der Verfasser der E-Mail versucht, diese mit dem Zertifikat zu signieren, wird eine Fehlernachricht angezeigt.	Verwenden Sie zur Auswahl des Zertifikats die Sicherheitseinstellungen in Netscape Messenger. Wenn Netscape Messenger geöffnet ist, klicken Sie in der Symbolleiste auf das Sicherheitssymbol. Das Fenster mit den Sicherheitsinformationen wird geöffnet. Klicken Sie im linken Teilfenster auf **Netscape Messenger**, und wählen Sie anschließend **Zertifikat des integrierten IBM Security Chips** aus. Weitere Informationen hierzu finden Sie in der Dokumentation von Netscape.
Eine E-Mail wird mit einem anderen Algorithmus an den Client zurückgesendet.	**Maßnahme**
Eine mit dem RC2(40)-, RC2(64)- oder RC2(128)-Algorithmus verschlüsselte E-Mail wird von einem Client mit Netscape Messenger an einen Client mit Outlook Express (128 Bit) gesendet. Eine vom Outlook Express-Client zurückgesendete E-Mail wird mit dem Algorithmus RC2(40) verschlüsselt.	Es ist keine Maßnahme erforderlich. Eine Verschlüsselungsanforderung gemäß RC2(40), RC2(64) oder RC2(128) von einem Netscape-Client an einen Outlook Express-Client (128 Bit) wird an den Netscape-Client immer mit dem RC2(40)-Algorithmus zurückgesendet. Aktuelle Informationen zu den Verschlüsselungsalgorithmen, die mit den verschiedenen Versionen von Outlook Express verwendet werden, erhalten Sie von Microsoft.

Fehlersymptom	Mögliche Lösung
Ein digitales Zertifikat, das vom integrierten IBM Security Chip generiert wurde, kann nicht verwendet werden.	**Maßnahme**
Das vom integrierten IBM Security Chip generierte digitale Zertifikat ist nicht verfügbar.	Überprüfen Sie, ob Sie beim Öffnen von Netscape den richtigen UVM-Verschlüsselungstext eingegeben haben. Wenn Sie den falschen UVM-Verschlüsselungstext eingeben, wird eine Fehlernachricht über einen Authentifizierungsfehler angezeigt. Wenn Sie auf **OK** klicken, wird Netscape geöffnet, Sie können aber das vom integrierten IBM Security Chip generierte Zertifikat nicht verwenden. Sie müssen Netscape verlassen und erneut öffnen und anschließend den richtigen UVM-Verschlüsselungstext eingeben.
Neue digitale Zertifikate vom selben Sender werden innerhalb von Netscape nicht ausgetauscht.	**Maßnahme**
Wenn eine digital signierte E-Mail vom selben Sender mehrmals empfangen wird, wird das erste digitale Zertifikat, das der E-Mail zugeordnet ist, nicht überschrieben.	Wenn Sie mehrere E-Mail-Zertifikate empfangen, ist das einzige Zertifikat das Standardzertifikat. Löschen Sie mit den Sicherheitseinrichtungen in Netscape das erste Zertifikat, und öffnen Sie anschließend das zweite Zertifikat erneut, oder bitten Sie den Sender, eine weitere signierte E-Mail zu senden.
Das Zertifikat des integrierten IBM Security Chips kann nicht exportiert werden.	**Maßnahme**
Das Zertifikat des integrierten IBM Security Chips kann in Netscape nicht exportiert werden. Die Exportfunktion in Netscape können Sie zum Sichern von Zertifikaten verwenden.	Rufen Sie das Administratordienstprogramm oder Benutzerkonfigurationsprogramm auf, um das Schlüsselarchiv zu aktualisieren. Wenn Sie das Schlüsselarchiv aktualisieren, werden von allen Zertifikaten, die dem integrierten IBM Security Chip zugeordnet sind, Kopien erstellt.
Beim Versuch, ein wiederhergestelltes Zertifikat nach dem Ausfall eines Festplattenlaufwerks zu verwenden, wird eine Fehlernachricht angezeigt.	**Maßnahme**
Zertifikate können im Administratordienstprogramm mit der Wiederherstellungsfunktion für Schlüssel wiederhergestellt werden. Möglicherweise sind einige Zertifikate, wie z. B. die kostenfreien Zertifikate von VeriSign, nach einer Schlüsselwiederherstellung nicht wiederhergestellt.	Fordern Sie nach dem Wiederherstellen der Schlüssel ein neues Zertifikat an.

Fehlersymptom	Mögliche Lösung
Der Netscape-Agent wird geöffnet und verursacht einen Fehler in Netscape.	**Maßnahme**
Das Öffnen des Netscape-Agenten führt zum Schließen von Netscape.	Schalten Sie den Netscape-Agenten aus.
Netscape wird mit zeitlicher Verzögerung geöffnet.	**Maßnahme**
Wenn Sie das PKCS #11-Modul des integrierten IBM Security Chips hinzufügen und anschließend Netscape öffnen, verzögert sich das Öffnen von Netscape um kurze Zeit.	Es ist keine Maßnahme erforderlich. Dies dient lediglich zu Ihrer Information.

Fehlerbehebungsinformationen zu digitalen Zertifikaten

Die folgenden Informationen zur Fehlerbehebung können hilfreich sein, wenn bei der Anforderung eines digitalen Zertifikats Fehler auftreten.

Fehlersymptom	Mögliche Lösung
Das Fenster "UVM-Verschlüsselungstext" oder das Fenster für die Authentifizierung über Fingerabdrücke wird bei der Anforderung eines digitalen Zertifikats mehrmals angezeigt.	**Maßnahme**
In der UVM-Sicherheits-Policy ist festgelegt, dass ein Benutzer sich mit einem UVM-Verschlüsselungstext oder über Fingerabdrücke authentifizieren muss, bevor er ein digitales Zertifikat erhalten kann. Wenn der Benutzer versucht, ein Zertifikat zu erhalten, wird das Authentifizierungsfenster, in dem er aufgefordert wird, den UVM-Verschlüsselungstext anzugeben oder die Fingerabdrücke abtasten zu lassen, mehrmals angezeigt.	Geben Sie bei jedem Öffnen des Authentifizierungsfensters den UVM-Verschlüsselungstext ein bzw. lassen Sie ihre Fingerabdrücke abtasten.
Eine Nachricht über einen VBScript- oder JavaScript-Fehler wird angezeigt.	**Maßnahme**
Wenn Sie ein digitales Zertifikat anfordern, wird möglicherweise eine Fehlernachricht angezeigt, die sich auf VBScript oder JavaScript bezieht.	Starten Sie den Computer erneut, und beziehen Sie das Zertifikat erneut.

Fehlerbehebungsinformationen zu Tivoli Access Manager

Die folgenden Informationen zur Fehlerbehebung können hilfreich sein, wenn bei der Verwendung von Tivoli Access Manager in Verbindung mit Client Security Fehler auftreten.

Fehlersymptom	Mögliche Lösung
Die lokalen Policy-Einstellungen entsprechen nicht denen auf dem Server.	**Maßnahme**
Tivoli Access Manager lässt bestimmte Bit-Konfigurationen zu, die von UVM nicht unterstützt werden. Folglich können lokale Policy-Anforderungen Einstellungen überschreiben, die ein Administrator bei der Konfiguration eines PD-Servers vorgenommen hat.	Dies ist eine bekannte Einschränkung.
Kein Zugriff auf die Konfigurationseinstellungen von Tivoli Access Manager	**Maßnahme**
Im Administratordienstprogramm kann auf der Seite zur Policy-Installation weder auf die Konfigurationseinstellungen von Tivoli Access Manager noch auf die entsprechenden Einstellungen zur lokalen Cache-Einrichtung zugegriffen werden.	Installieren Sie Tivoli Access Manager Runtime Environment. Wenn die Laufzeitumgebung (Runtime Environment) auf dem IBM Client nicht installiert ist, sind auf der Seite zur Policy-Installation auch keine Einstellungen für Tivoli Access Manager verfügbar.
Eine Benutzersteuerung gilt sowohl für den Benutzer als auch für die Gruppe.	**Maßnahme**
Wenn Sie beim Konfigurieren des Tivoli Access Manager-Servers einen Benutzer für eine Gruppe definieren, gilt die Benutzersteuerung sowohl für den Benutzer als auch für die Gruppe, wenn die Option **Traversebit** aktiviert wurde.	Es ist keine Maßnahme erforderlich.

Fehlerbehebungsinformationen zu Lotus Notes

Im folgenden Abschnitt finden Sie Informationen, die Ihnen bei der Behebung von Fehlern bei der Verwendung von Lotus Notes mit Client Security weiterhelfen können.

Fehlersymptom	Mögliche Lösung
Nach dem Aktivieren des UVM-Schutzes für Lotus Notes kann Lotus Notes die Konfiguration nicht fertig stellen.	**Maßnahme**
Lotus Notes kann nach dem Aktivieren des UVM-Schutzes mit dem Administratordienstprogramm die Konfiguration nicht fertig stellen.	Dies ist eine bekannte Einschränkung. Lotus Notes muss konfiguriert werden und aktiv sein, bevor die Lotus Notes-Unterstützung im Administratordienstprogramm aktiviert wird.
Beim Versuch, das Notes-Kennwort zu ändern, wird eine Fehlernachricht angezeigt.	**Maßnahme**
Wenn Sie das Notes-Kennwort bei Verwendung von Client Security ändern, wird dies in einer Fehlernachricht angezeigt.	Wiederholen Sie die Kennwortänderung. Wurde der Fehler dadurch nicht behoben, starten Sie den Client neu.
Nach dem Festlegen eines Kennworts per Zufallsgenerator wird eine Fehlernachricht angezeigt.	**Maßnahme**
Wenn Sie folgende Vorgänge ausführen, wird möglicherweise eine Fehlernachricht angezeigt: • Verwenden des Tools zur Lotus Notes-Konfiguration zur Einstellung des UVM-Schutzes für eine Notes-ID • Öffnen von Notes und Verwenden der Notes-Funktion zur Kennwortänderung für die Datei mit der Notes-ID • Schließen von Notes sofort nach der Kennwortänderung	Klicken Sie auf **OK**, um die Fehlernachricht zu schließen. Es ist keine weitere Maßnahme erforderlich. Entgegen der Fehlernachricht wurde das Kennwort geändert. Das neue Kennwort wurde von Client Security per Zufallsgenerator festgelegt. Die Datei mit der Notes-ID wird nun mit dem per Zufallsgenerator festgelegten Kennwort verschlüsselt, und der Benutzer benötigt keine neue Benutzer-ID-Datei. Wenn der Endbenutzer das Kennwort erneut ändert, generiert UVM ein neues, per Zufallsgenerator festgelegtes Kennwort für die Notes-ID.

Fehlerbehebungsinformationen zur Verschlüsselung

Im folgenden Abschnitt finden Sie Informationen, die Ihnen bei der Behebung von Fehlern bei der Verschlüsselung von Dateien unter Verwendung von Client Security ab Version 3.0 weiterhelfen können.

Fehlersymptom	Mögliche Lösung
Bereits verschlüsselte Dateien werden nicht entschlüsselt.	**Maßnahme**
Dateien, die mit früheren Versionen von Client Security verschlüsselt wurden, werden nach dem Upgrade auf Client Security ab Version 3.0 nicht entschlüsselt.	Dies ist eine bekannte Einschränkung. Sie müssen alle mit früheren Versionen von Client Security verschlüsselten Dateien entschlüsseln, *bevor* Sie Client Security ab Version 3.0 installieren. Client Security 3.0 kann Dateien, die von früheren Versionen von Client Security verschlüsselt wurden, nicht entschlüsseln, da in dieser Version die Implementierung der Dateiverschlüsselung geändert wurde.

Fehlerbehebungsinformationen zu UVM-sensitiven Einheiten

Im folgenden Abschnitt finden Sie Informationen, die Ihnen bei der Behebung von Fehlern bei der Verwendung UVM-sensitiver Einheiten weiterhelfen können.

Fehlersymptom	Mögliche Lösung
Eine UVM-sensitive Einheit funktioniert nicht mehr ordnungsgemäß.	**Maßnahme**
Wenn Sie eine UVM-sensitive Einheit vom USB-Anschluss (Universal Serial Bus) trennen und die Einheit danach erneut am USB-Anschluss anschließen, funktioniert die Einheit möglicherweise nicht ordnungsgemäß.	Starten Sie nach dem erneuten Anschluss der Einheit an den USB-Anschluss den Computer erneut.

Anhang A. Regeln für Kennwörter und Verschlüsselungstexte

In diesem Anhang finden Sie Informationen zu den Regeln für verschiedene Systemkennwörter.

Regeln für Hardwarekennwörter

Für Hardwarekennwörter gelten die folgenden Regeln:

Länge Das Kennwort muss genau acht Zeichen lang sein.

Zeichen
Das Kennwort darf nur alphanumerische Zeichen enthalten. Die Kombination von Buchstaben und Ziffern ist zulässig. Es sind keine speziellen Zeichen wie das Leerzeichen und die Zeichen !, ?, % zulässig.

Merkmale
Sie können das Kennwort für den IBM Security Chip festlegen, um den integrierten IBM Security Chip im Computer zu aktivieren. Dieses Kennwort müssen Sie bei jedem Zugriff auf das Administratordienstprogramm eingeben.

Fehlversuche
Wenn Sie das Kennwort zehnmal falsch eingegebenen haben, wird der Computer 1 Stunde und 17 Minuten lang gesperrt. Wenn Sie nach diesem Zeitraum das Kennwort zehn weitere Male falsch eingeben, wird der Computer 2 Stunden und 34 Minuten lang gesperrt. Die Dauer der Computersperrung verdoppelt sich jedes Mal, wenn Sie das Kennwort zehnmal falsch eingeben.

Regeln für UVM-Verschlüsselungstexte

Die Sicherheit wird dadurch erhöht, dass der UVM-Verschlüsselungstext länger und eindeutiger ist als ein herkömmliches Kennwort. Die Policy für den UVM-Verschlüsselungstext wird über das Administratordienstprogramm von IBM Client Security gesteuert.

Das Fenster ″Policy für UVM-Verschlüsselungstext″ des Administratordienstprogramms stellt Sicherheitsadministratoren eine einfache Schnittstelle zur Steuerung von Kriterien für Verschlüsselungstexte bereit. Über das Fenster ″Policy für UVM-Verschlüsselungstext″ kann der Administrator folgende Regeln für Verschlüsselungstexte festlegen:

Anmerkung: Die Standardeinstellung für jedes Kriterium ist unten in Klammern angegeben.

- ob eine Mindestanzahl an alphanumerischen Zeichen festgelegt werden soll (ja, 6)

  Wenn z. B. der Wert ″6″ festgelegt ist, ist der Verschlüsselungstext `1234567xxx` ungültig.
- ob eine Mindestanzahl an Ziffern festgelegt werden soll (ja, 1)

  Wenn z. B. der Wert ″1″ festgelegt ist, ist der Verschlüsselungstext `thisismypassword` ungültig.

- ob eine Mindestanzahl an Leerzeichen festgelegt werden soll (keine Mindestanzahl)

  Wenn z. B. der Wert ″2″ festgelegt ist, ist der Verschlüsselungstext `i am not here` ungültig.
- ob mehr als zwei wiederkehrende Zeichen zulässig sein sollen (nein)

  Wenn dies z. B. festgelegt ist, ist der Verschlüsselungstext `aaabcdefghijk` ungültig.
- ob der Verschlüsselungstext mit einer Ziffer beginnen darf (nein)

  Standardmäßig ist z. B. der Verschlüsselungstext `1password` ungültig.
- ob der Verschlüsselungstext mit einer Ziffer enden darf (nein)

  Standardmäßig ist z. B. der Verschlüsselungstext `password8` ungültig.
- ob der Verschlüsselungstext eine Benutzer-ID enthalten darf (nein)

  Standardmäßig ist z. B. der Verschlüsselungstext `Benutzername` ungültig, wobei es sich bei `Benutzername` um eine Benutzer-ID handelt.
- ob der neue Verschlüsselungstext sich von den letzten x Verschlüsselungstexten unterscheiden muss (ja, 3)

  Standardmäßig ist z. B. der Verschlüsselungstext `mypassword` ungültig, wenn einer der drei vorherigen Verschlüsselungstexte `mypassword` war.
- ob der Verschlüsselungstext mehr als drei identische aufeinander folgende Zeichen des letzten Kennworts enthalten darf (nein)

  Standardmäßig ist z. B. der Verschlüsselungstext `password` ungültig, wenn einer der drei vorherigen Verschlüsselungstexte `pass` oder `word` war.

Das Fenster ″Policy für UVM-Verschlüsselungstext″ des Administratordienstprogramms ermöglicht Sicherheitsadministratoren zudem eine Steuerung des Ablaufs der Verschlüsselungstexte. Über das Fenster ″Policy für UVM-Verschlüsselungstext″ kann der Administrator aus den folgenden Regeln für Verschlüsselungstexte auswählen:

- Verschlüsselungstext ist nicht mehr gültig nach (ja, 184).

  In diesem Beispiel läuft der Verschlüsselungstext standardmäßig nach 184 Tagen ab. Der neue Verschlüsselungstext muss der vorhandenen Policy für den Verschlüsselungstext entsprechen.
- Verschlüsselungstext läuft nie ab.

  Wenn diese Option ausgewählt ist, läuft der Verschlüsselungstext nie ab.

Die Policy für den Verschlüsselungstext wird vom Administratordienstprogramm bei der Registrierung des Benutzers und bei der Änderung des Verschlüsselungstextes durch den Benutzer über das Clientdienstprogramm überprüft. Die beiden Benutzereinstellungen zum vorherigen Kennwort werden zurückgesetzt, und Protokolle zum Verschlüsselungstext werden entfernt.

Folgende allgemeine Regeln gelten für UVM-Verschlüsselungstexte:

Länge Der Verschlüsselungstext kann bis zu 256 Zeichen lang sein.

Zeichen
: Der Verschlüsselungstext kann jede beliebige Kombination von Zeichen enthalten, die die Tastatur erzeugt, einschließlich Leerzeichen und nicht alphanumerische Zeichen.

Merkmale

Der UVM-Verschlüsselungstext unterscheidet sich von einem Kennwort, das Sie zur Anmeldung am Betriebssystem verwenden können. Der UVM-Verschlüsselungstext kann in Verbindung mit anderen Authentifizierungseinheiten verwendet werden, z. B. mit einem UVM-Sensor für Fingerabdrücke.

Fehlversuche

Wenn Sie während einer Sitzung den UVM-Verschlüsselungstext mehrmals falsch eingeben, wird der Computer nicht gesperrt. Für die Anzahl der Fehlversuche besteht keine Begrenzung.

Anhang B. Regeln für den UVM-Schutz für die Anmeldung am System

Mit dem UVM-Schutz wird sichergestellt, dass nur Benutzer, die in UVM für einen bestimmten IBM Client hinzugefügt wurden, auf das Betriebssystem zugreifen können. Windows-Betriebssysteme umfassen Anwendungen, die einen Anmeldeschutz bieten. Auch wenn UVM-Schutz parallel mit diesen Windows-Anmeldeanwendungen verwendet werden kann, funktioniert er je nach Betriebssystem etwas anders.

Die UVM-Anmeldeschnittstelle ersetzt die Anmeldung am Betriebssystem, so dass immer wenn sich ein Benutzer am System anmelden möchte, das UVM-Anmeldefenster angezeigt wird.

Lesen Sie die folgenden Hinweise, bevor Sie den UVM-Anmeldeschutz für das System konfigurieren und verwenden:

- Löschen Sie den Inhalt des integrierten IBM Security Chips nicht bei aktiviertem UVM-Schutz. Andernfalls wird der Inhalt der Festplatte unbrauchbar, und Sie müssen die Festplatte neu formatieren und die gesamte Software neu installieren.
- Wenn Sie im Administratordienstprogramm das Markierungsfeld **Die Windows-Standardanmeldung durch eine gesicherte UVM-Anmeldung ersetzen** inaktivieren, kehrt das System zum Windows-Anmeldungsprozess zurück, ohne die gesicherte UVM-Anmeldung zu verwenden.
- Sie haben die Option, die maximale Anzahl der Versuche für die Eingabe des richtigen Kennworts für die Windows-Anmeldeanwendung anzugeben. Diese Option steht bei UVM-Anmeldeschutz *nicht* zur Verfügung. Für die Anzahl der zulässigen Fehlversuche bei der Eingabe des UVM-Verschlüsselungstextes können Sie keine Grenze festlegen.

Anhang C. Bemerkungen und Marken

Dieser Anhang enthält rechtliche Hinweise zu IBM Produkten und Informationen zu Marken.

Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden.

Möglicherweise bietet IBM die in diesem Dokument beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Dienstleistungen von IBM verwendet werden können. Anstelle der Produkte, Programme oder Dienstleistungen können auch andere, ihnen äquivalente Produkte, Programme oder Dienstleistungen verwendet werden, solange diese keine gewerblichen oder andere Schutzrechte von IBM verletzen. Die Verantwortung für den Betrieb von Fremdprodukten, Fremdprogrammen und Fremddienstleistungen liegt beim Kunden.

Für in diesen Dokument beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder IBM Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanfragen sind schriftlich an folgende Adresse zu richten (Anfragen an diese Adresse müssen auf Englisch formuliert werden):

IBM Europe
Director of Licensing
92066 Paris
La Defense, Cedex
France

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die Angaben in diesem Handbuch werden in regelmäßigen Zeitabständen aktualisiert. Die Änderungen werden in Überarbeitungen oder in Technical News Letters (TNLs) bekannt gegeben. IBM kann jederzeit ohne Vorankündigung Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängigen, erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse: IBM Corporation, Department 80D, P.O. Box 12195, 3039 Cornwallis, Research Triangle Park, NC 27709, U.S.A. Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des in diesem Dokument aufgeführten Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt im Rahmen der Allgemeinen Geschäftsbedingungen der IBM, der Internationalen Nutzungsbedingungen der IBM für Programmpakete oder einer äquivalenten Vereinbarung.

Marken

IBM und SecureWay sind in gewissen Ländern Marken der IBM Corporation.

Tivoli ist in gewissen Ländern eine Marke von Tivoli Systems Inc.

Microsoft, Windows und Windows NT sind in gewissen Ländern Marken der Microsoft Corporation.

Andere Namen von Unternehmen, Produkten und Dienstleistungen können Marken oder Dienstleistungsmarken anderer Unternehmen sein.